



Portalverbundprotokoll Version 2 Allgemeiner Teil		Konvention				
		PVP2-2.0.0				
		Empfehlung				
Kurzbeschreibung	<p>Das Portalverbundsystem ermöglicht das Zusammenwirken von Stammportalen zur Registrierung von Benutzern mit ihren Zugriffsrechten einerseits und Anwendungsportalen zur Überprüfung des berechtigten Zuganges zu Anwendungen andererseits.</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> <p>Die Version 2 des Portalverbundprotokolls unterstützt mehrere Profile, wie das Reverse-Proxy-Profil entsprechend der Versionen 1.x, und das SAML2 konforme „Redirect“ Profil.</p>					
Autor(en):	Peter Pfläging (Wien) Rainer Hörbe (Wien)	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">Projektteam / Arbeitsgruppe</td> </tr> <tr> <td style="text-align: center;">AG Integration und Zugänge (AG-IZ)</td> </tr> <tr> <td style="text-align: center;">AG-Leiter: Peter Pfläging (Wien)</td> </tr> <tr> <td style="text-align: center;">Stellvertreter: D.I. Peter Reichstädter (BKA)</td> </tr> </table>	Projektteam / Arbeitsgruppe	AG Integration und Zugänge (AG-IZ)	AG-Leiter: Peter Pfläging (Wien)	Stellvertreter: D.I. Peter Reichstädter (BKA)
Projektteam / Arbeitsgruppe						
AG Integration und Zugänge (AG-IZ)						
AG-Leiter: Peter Pfläging (Wien)						
Stellvertreter: D.I. Peter Reichstädter (BKA)						
Beiträge von:	Peter Pichler, Joachim Minichshofer					

Version 2.0.0 : **31.8.2011**

Angenommen: **14.10.2011**

VST-1712/455

Inhaltsverzeichnis

1 Über das Dokument und die Protokollversionen	4
1.1 Versionsnummern für PVP2	4
1.2 Beispiele für Versionsnummern.....	4
2 Zweck.....	6
3 Schreibweise.....	7
3.1 Normative und nicht-normative Teile	7
3.2 Begriffsbestimmung.....	7
3.2.1 Application Chaining.....	7
3.2.2 Subteilnehmer	7
3.2.3 Participant.....	7
3.2.4 Verrechnungsdaten	7
3.2.5 Identity Provider (IdP), Service Provider (SP), Attribute Provider	7
3.3 Vergleiche zu anderen Nomenklaturen	7
4 Architektur.....	9
4.1 Basisprofile	9
4.1.1 Basisprofil R (Reverse Proxy Profil).....	9
4.1.2 Basisprofil S (SAML Web-SSO Profil).....	9
4.1.3 Geplant: Basisprofil X (IHE XUA Cross Enterprise User Authentication).....	9
4.1.4 Geplant: Basisprofil O (OpenID)	10
4.2 Key Bindings	10
4.3 Akteure	11
4.4 Message Sequenz.....	11
5 PVP eGovToken: Das eGovernment Attribute Profile	12
5.1 Änderungen gegenüber dem PVP 1.9 PVP-Token	12
5.2 Attribute Profile.....	13
5.2.1 Fremde Namensräume	13
5.3 PVP2 Attribute.....	14
5.3.1 Syntaxangaben / Augmented BNF	14
5.3.2 BNF Syntax.....	14
5.3.3 Abbildung von PVP2 zu PVP1	14
5.3.4 OIDs für Attribute der PVP Spezifikation	14
5.3.5 Listenattribute	15
5.3.6 Attributverzeichnis	16
5.3.6.1 Technische Informationen	16
PVP-eGovTokenVersion	16
5.3.6.2 Namen.....	17
principal Name.....	17
Vorname (givenName)	18
OID	18
5.3.6.3 Identifikationskennzeichen	19
Benutzerkennung (userId).....	19
Globale Account Kennung (gid).....	20
Bereichsspezifische Personenkennung (gvpPK).....	21
5.3.6.4 Organisatorische Zugehörigkeiten	22
Kennung des Verbundteilnehmers (participantId)	22
Organisationskennzeichen der Organisationseinheit (ouOKZ).....	23

gvOuid der Organisationseinheit (ouGvOuid).....	24
Kurzbezeichnung der Organisationseinheit (ou).....	25
Funktionsbezeichnung (function).....	26
5.3.6.5 Kontaktinformationen.....	27
E-Mail Adresse (mail)	27
Telefonnummer (tel)	28
5.3.6.6 Sicherheitsklasse des Principals.....	29
PVP-eGovTokenVersion	29
5.3.6.7 Berechtigungen / Autorisierung / Rollen	30
Roles (roles).....	30
5.3.6.8 Verrechnungsrelevante Informationen.....	31
Rechnungsempfänger (invoiceRecptId).....	31
Kostenstellen (costCenterId).....	32
Gebührenstufe (chargeCode).....	33
5.3.6.9 Reverse-Proxy Profil spezifische Parameter	34
Transaktionskennung (txid)	34
URL der Transaktion wie vom Client benutzt: Schema	35
URL der Transaktion wie vom Client benutzt: Host	36
URL der Transaktion wie vom Client benutzt: URI	37
5.3.7 Application Chaining.....	38
5.3.7.1 Allgemeines / Chained-Token	38
5.3.7.2 Chained Token in SAML Profilen.....	39
5.3.7.3 Attribute des Chained-Tokens.....	39
5.3.8 Chained-Token-Num-ID.....	39
5.3.9 Exkurs: IDs für Organisationen und OE im österr. E-Government	40
5.3.9.1 Kennzeichen nach der Spezifikation VKZ.....	40
5.3.9.2 Kennzeichen nach ldap.gv.at	41
gvOuid	41
gvOuidVKZ.....	41
5.3.9.3 Zusammenfassung.....	42
Anhang A Beispiele für Rechte und Rechteparameter.....	43
Einfaches Berechtigungschema	43
Komplexeres Berechtigungschema	43
Anhang B Referenzen.....	44

1 Über das Dokument und die Protokollversionen

PVP2 ist eine Standardisierungsbestrebung, die es erlaubt auf Basis der Rahmenspezifikation und des Datenmodells unterschiedliche Protokollbindungen in mehreren Ebenen zu implementieren. Dabei kann zum Beispiel sowohl SOAP kompatibler Inhalt auf der Ebene der Reverse Proxy Protokollbindung als auch auf einer SAML2 kompatiblen Redirect Bindung implementiert werden.

Dokumente der PVP 2 Spezifikation:

- **PVP2-Allgemein** ist das Basisdokument, welches folgende Elemente enthält:
 - a) Allgemeiner Teil mit Erklärungen und Zweckdefinition
 - b) Die Beschreibung der notwendigen Nomenklatur und der Schreibweisen
 - c) Die Architektur des Portalverbundprotokolls
 - d) Das Datenmodell, welches allen Protokollvarianten zu Grunde liegt
 - e) Die Anhänge
- **PVP2-R-Profil** ist die Weiterführung der PVP 1.x Reverse Proxy Protokollvarianten. Das betrifft sowohl die HTTP/HTML Bindung als auch die SOAP Protokollbindung
- **PVP2-S-Profil** entspricht der Spezifikation des SAML2 Web-SSO-Profiles.

1.1 Versionsnummern für PVP2

Aufgrund der Tatsache, dass in PVP2 mehrere Protokollvarianten auf einer gemeinsamen Basis implementiert wurden, ist es sinnvoll die Versionsnummerierung dieser Tatsache anzupassen, da sonst bei minimalen Änderungen einer Protokollimplementierung sämtliche anderen Protokollversionen geändert werden müssen, ohne dass es tatsächliche Änderungen gibt.

Um die Vereinheitlichung der Dokumentkonventionen¹ in seiner 3 stufigen Versionsnummerierung zu erhalten wird daher folgende Vorgangsweise verwendet:

Das Hauptdokument **PVP2-Allgemein** behält die normale Versionsnummerierung wie in der oben genannten Dokumentkonvention:

a.b.c – wobei a die Hauptversion, b die Unterversion und c die Nummer des Fehlerkorrekturlevels darstellt.

Die **PVP-...-Profil** Dokumente folgen immer exakt der Nomenklatur des zugehörigen PVP2-Allgemein – Dokumentes, hängen aber eine weitere Stelle mit einem Buchstaben (beginnend mit „a“) an, der die Unterversion der Protokollbindungsvariante bezeichnet. Wird das Hauptdokument um eine Version erhöht, so werden alle aktuellen Versionen der Protokollbindungen gesetzt auf: Hauptprotokollversion „a“.

¹ http://reference.e-government.gv.at/KOOP_e-gov-koop_2_0_2_13_9.916.0.html

1.2 Beispiele für Versionsnummern

PVP2-Allgemein-2.37.14
PVP2-R-Profil Profile-2.37.14.a
PVP2-S-Profil-2.37.14.f

Die nächsten Versionen der Teildokumente wären demnach:
PVP2-R-Profil-2.37.14.b oder
PVP2-S-Profil-2.37.14.g

Ändert sich an der Spezifikation PVP2-Allgemein etwas würde sich folgendes Bild ergeben:

PVP2-Allgemein-2.38.0
PVP2-R-Profil-2.38.0.a
PVP2-S-Profil-2.38.0.a

D.h. es hat sich zumindest in der Basisversion etwas geändert, und damit sind auch alle –Profil Versionen zu berücksichtigen und erhalten eine neue Versionsnummer.

Der komplette Dokumentensatz soll als ZIP-Archiv zur Verfügung gestellt werden. In dieser ZIP Datei sollte eine ReadMe Datei die aktuellen Versionen aufführen und die ZIP Datei eine stetig steigende Build Number im Dateinamen enthalten. In unserem Beispiel wären das:

PVP2-2.37.14.251 bzw. PVP2-2.38.0.394

2 Zweck

Das Portalverbundsystem ermöglicht die Delegation von Identitätsprüfung, Authentifizierung und Autorisierung [PV-Whitepaper]. Das Protokoll erweitert die Kommunikation zwischen Stamm- und Anwendungsportalen, indem vertrauenswürdige Aussagen über Authentizität, Autorisierung und Verrechnungsdaten von Benutzern kommuniziert werden.

Autorisierung bedeutet in diesem Zusammenhang, dass einem Benutzer für den Zugriff auf eine Ressource Rechte, Rechteparameter und eine Sicherheitsklasse zugewiesen werden.

Die Kommunikation zwischen den Portalen muss Integrität und Vertraulichkeit gewährleisten.

Der Portalverbund (PV) im Sinne von [PVV 1.0] ist zur Kommunikation zwischen Körperschaften öffentlichen Rechts vorgesehen. Für den Verbund sind rechtliche, organisatorische und technische Ebenen relevant, daher sind neben dieser technischen Protokollspezifikation weitere Dokumente wie die Portalverbundvereinbarung [PVV] und Sicherheitsklassen [SecClass] zu beachten. Das Protokoll kann aber in einem anderen rechtlichen Kontext für weitere Zwecke verwendet werden:

- Kommunikation zwischen Behörden und Nicht-Behörden auf Grund bilateraler Vereinbarungen
- Kommunikation zwischen internen Stamm- und Anwendungsportalen
- Kommunikation zwischen Anwendungsportalen und Anwendungen
- Kommunikation in anderen Verbänden (z.B. Wirtschaftsportalverbund)

3 Schreibweise

3.1 Normative und nicht-normative Teile

Beispiele und Fußnoten sind nicht Teil der Spezifikation.

3.2 Begriffsbestimmung

Die Begriffe sind in [PVV 1.0] definiert. Ergänzend dazu wird festgelegt:

3.2.1 Application Chaining

Das ist der Fall, wenn der Zugriff eines Benutzers auf eine Anwendung im Umweg über eine oder mehrere andere Anwendung(en) erfolgt.

3.2.2 Subteilnehmer

Bezeichnet eine Organisation, die mittels der Vereinbarung (inkl. der Verpflichtung zur Einhaltung von [PV-DASI] über einen Teilnehmer am Portalverbund teilnimmt.

3.2.3 Participant

Bezeichnet jene zugriffsberechtigte Stelle, die ein Teilnehmer oder ein Subteilnehmer im Verwaltungsportalverbund ist. Ein Participant muss eine Rechtsperson sein, kann also keine Organisationseinheit sein.

3.2.4 Verrechnungsdaten

bestehen aus der Identifikation des Rechnungsempfängers, und der Liste der möglichen Kostenstellen und Gebührenstufen des Anwenders. Die Auswahl der konkreten Kostenstelle und Gebührenstufe einer Transaktion erfolgt in der Anwendung, nicht im PVP.

3.2.5 Identity Provider (IdP), Service Provider (SP), Attribute Provider

Sind in [AG-IZ Glossar] definiert.

3.3 Vergleiche zu anderen Nomenklaturen

Im [AG-IZ Glossar] sind weitere Referenzen auf andere Standards enthalten.

<i>PVP1</i>	<i>SAML</i>	<i>RFC 2904</i>	<i>PVP2</i>
Anwendung	Service Provider	Service Equipment	Service Provider
Anwendungsportal		AAA-Server (Org1)	
Portalverbund	Circle of Trust	(agreement)	Portalverbund
Benutzer	Client	User	Principal
Stammportal	Identity Provider	AAA-Server (Org2)	Identity Provider, Attribute Provider
zugriffsberechtigte Stelle		User Home Organization	Stammorganisation

4 Architektur

4.1 Basisprofile

Die Versionen des Portalverbundprotokolls beginnend mit Version 2.0 spezifizieren unterschiedliche Basisprofile in denen die Attribute der authentifizierten Benutzer und Systeme (Organisationszugehörigkeit, übertragene Rechte, transaktionsbezogene Verrechnungsdaten) kompatibel abgebildet werden.

Was sich jedoch ändert ist die Art des Transports der Informationen und das Kommunikationsmuster.

Es sind derzeit die Basisprofile R-Profil und S-Profil spezifiziert:

4.1.1 Basisprofil R (Reverse Proxy Profil)

Das „R“ Profil im PVP ist eine Fortführung des klassischen PVP1-Protokolls, indem ein Stammportal den Benutzer authentifiziert, seine Rechte definiert und anschließend den HTTP-Request in einer „Reverse Proxy“ Methode weiterreicht.

Das R-Profil hat auch eine SOAP-Bindung, die sowohl als Reverse-Proxy als auch direkt² verwendet werden kann.

4.1.2 Basisprofil S (SAML Web-SSO Profil)

Das „S“ Profil implementiert eine Variante des SAML 2 Web-SSO Profils, indem die Identifikation über einen Identity Provider (IdP) abgewickelt wird und anschließend eine Umleitung unter Mitgabe der Logon Informationen zum Service Provider (Applikation bzw. Anwendungsportal in PVP1 Nomenklatur) erfolgt.

Vor- und Nachteile der Basisprofile

Feature	R-Profil	S-Profil
Einbindung über VPN/IP-Adresseinschränkung	Einfacher durch beschränkte Anzahl von Stammportalen	Clients müssten über eigenes VPN oder Ähnliches gehen
Datenschutz	Stammportal liest Verkehr (Inhalt) mit	IdP erfährt nur die Authentifizierungsanfragen
Application Proxy	Für Sicherheit von DMZ sinnvoll	Müsste extra konfiguriert werden
Starkes Key Binding (→4.2)	nein	möglich
Anwendungskompatibilität	Relative ULRs, definierter Namespace	Keine speziellen Erfordernisse
Anwendungsschnittstelle	PVP	SAML

² Bei einem direkten Zugriff authentifiziert sich der WS-Client wie ein Stammportal und benötigt daher keinen Reverse Proxy.

4.1.3 Geplant: Basisprofil X (IHE XUA Cross Enterprise User Authentication)

Für die SOAP-Bindung nach dem WS-Security Standard ist geplant das IHE XUA Profil zu verwenden, das im Gesundheitsbereich als strategischer Standard gilt.

4.1.4 Geplant: Basisprofil O (OpenID)

Als Alternative zum S-Profil ist das verbreitete OpenID-Protokoll geplant, das in vielen Produkten implementiert ist und auch von SaaS-Diensten häufig angeboten wird.

4.2 Key Bindings

Aus der SAML-Welt kommend werden für Authentifizierungsprotokolle drei Arten definiert mit der die Inhalte der Transaktion, Benutzerattribute und Schlüssel zu einem Sicherheitskontext verbunden werden:

1. Holder of Key: Der Principal authentifiziert seine Attribute mit seinem eigenen privaten Schlüssel. Häufig wird auch gefordert, dass der Transportkanal (TLS) an diesen Schlüssel gebunden sein muss. Beispiel: Vom Principal signierte SAML-Assertion.
2. Sender Vouches: Ein Reverse Proxy verwendet seinen privaten Schlüssel um die Identität eines Principals zu authentifizieren. Beispiel: Ein SOAP-Gateway signiert einen Request von einem am Gateway authentifizierten Principal.
3. Bearer: Die im Request enthaltene Identität wird in einem gesicherten Kanal übermittelt, ist aber nicht direkt an den Schlüssel gebunden. Beispiel: Attribute die über TLS oder eine lokale Systemschnittstelle übermittelt werden.

Die Basisprofile ermöglichen folgende Key Bindings:

	Holder-of-Key	Sender-Vouches	Bearer
R-Profil (HTTP)			X
R-Profil (SOAP)			X
S-Profil	X	X	X
X-Profil	X	X	
O-Profil		(X)	X

Bei R-Profil ist das Token durch die Übermittlung über TLS an den Schlüssel des IdP/Stammportals gebunden.

Beim S-Profil sind mehrere Konfigurationen möglich. Üblich ist die Übermittlung von SAML-Assertions die durch den IdP signiert sind - also „Sender-Vouches“. Holder-of-Key ist die sicherheitstechnisch stärkste Variante weil der Sicherheitskontext über die Dauer der Session kryptografisch gesichert ist. Beim Bearer-Token besteht die Abhängigkeit der technischen Bindung zwischen Kanal und Benutzeridentität wodurch etwa eine Verwundbarkeit in Bezug auf Man-in-the-middle Angriffe entsteht.

4.3 Akteure

Im Kontext des Portalverbunds besteht die Rechtsbeziehung nur zwischen IdP und SP (PVP1: Stamm- und Anwendungsportal). Die im PVP definierten Attribute beziehen sich auch auf Principals (Endbenutzer).

Für das Protokoll sind folgende Entitäten erforderlich:

- Principal (User- oder System Principal)
- IdP (Stammportal)
- SP (Anwendungsportal)

4.4 Message Sequenz

Der Portalverbund ist grundsätzlich neutral gegenüber dem Modell der Interaktionen zwischen Benutzern, Portalen und Anwendungen.

Für das PVP R-Profil ist derzeit jedoch ein Reverse Proxy-Modell vorgesehen, wie es im RFC 2904 Abschnitt 3.1.1 als „agent sequence“ definiert ist.

Das PVP S-Profil dagegen orientiert sich am SAML 2.0 WEB-SSO-Profil und implementiert daher eine Redirect Methode für die Anmeldeungssequenz.

5 PVP eGovToken: Das eGovernment Attribute Profile

Das hier spezifizierte Datenmodell für den Verwaltungsportalverbund wird über die verschiedenen Profile einheitlich umgesetzt um Interoperabilität über Gateways zu gewährleisten.

Mit PVP Attributen werden den SP in normierter Form Informationen über die angemeldeten Benutzer zur Verfügung gestellt. Für andere Anwendungsfälle als der Kommunikation zwischen Verwaltungseinheiten und ihren Organen sind nach dem Bedarf der Anwendungen und dem Prinzip der Datenminimierung andere Datenmodell zu definieren.

Die verschiedenen Attribute können in folgende Klassen eingeteilt werden:

- Technische Informationen (PVP eGovToken Version, Transaktions-ID)
- Sicherheitsklasse
- Namen (Principal name, Given Name)
- Benutzerkennungen (UserId, gvGid, bPK)
- Organisatorische Zugehörigkeiten (participantId, ou-OKZ, ouGvOuid)
- Kontaktinformationen (mail, tel)
- Autorisierungsinformationen (roles)
- Verrechnungsinformationen. (invoiceRcptId, costCenterId, chargeCode)

Die tatsächliche Strukturierung hängt vom jeweiligen Profil ab:

-
- Beim R-Profil mit SOAP-Bindung ist die Hierarchie durch das XML Schema vorgegeben
- Beim S-Profil werden die Attribute ohne Hierarchie in ein SAML Attribute Statement gepackt.

Diese Struktur hat aber keine Bedeutung bei der Verwendung der Attribute.

Die in PVP1 definierte, aber nicht genutzte Möglichkeit eine organisatorische Zuordnung für die Autorisierung mittels X-AUTHORIZE-OU/-OUID/-OUOKZ anzugeben wird in PVP2 nicht mehr unterstützt.

5.1 Änderungen gegenüber dem PVP 1.9 PVP-Token

Mit der Version 2 wurde folgende Änderungen umgesetzt (nicht normativ):

- Die Protokollversion bezieht sich nur mehr auf das PVPeGovToken
- Die Attribute haben keine Hierarchie mehr (AUTHENTICATE, AUTHORIZE, ..)
- Einfache Kennzeichnung von Pflichtattributen: In PVP 1.x wurden durch XML bzw die EBNF-Beschreibung komplexere Regeln ermöglicht, z.B. dass Account-Attribute gemeinsam oder gar nicht angegeben werden mussten. Das ist praktisch wenig relevant und wird mit v2.0 aufgegeben
- Refactoring der Attribut-Namen zu X-PVP-...
- Erweiterung des Zeichensatzes für Namen von druckbarem ISO-Latin auf druckbares Unicode. Im R-Profil müssen Nicht-ASCII Zeichen mit Numerischen-Entity-Referenzen übermittelt werden.
- Einheitliche Namen für HTTP-Bindung und SAML
- Trennung von Vor- und Nachnamen, da manche Anwendungen das in der Vergangenheit benötigt haben und die automatische Zerlegung nicht zu 100% funktioniert.

- Nur mehr eine Organisationsbindung (bisher gab es theoretisch je eine in X-Authenticate und X-Authorize.
- Diverse Detailänderungen bei den Attributen

5.2 Attribute Profile

Für die Übermittlung der PVP Attribute wird das SAML 2.0 X.500/LDAP Attribute Profile verwendet.

Profil-Identifikation: urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500

5.2.1 Fremde Namensräume

Präfix	Namensraum	Anmerkung
saml:	urn:oasis:names:tc:SAML:2.0:assertion	SAML 2.0 Assertion Namensraum, siehe auch [SAML20]
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	SAML 2.0 Namensraum, siehe auch [SAML20]
ds:	http://www.w3.org/2000/09/xmldsig#	Namespace aus XML Signature Syntax and Processing specification [XMLSig] und dem dazugehörenden Schema [XMLSig-XSD]
xenc:	http://www.w3.org/2001/04/xmlenc#	Namensraum der XML Encryption Syntax and Processing specification [XMLEnc] und dem dazugehörenden XML Schema [XMLEnc-XSD]
xs:	http://www.w3.org/2001/XMLSchema	XML Schema Namensraum
xsi:	http://www.w3.org/2001/XMLSchemainstance	XML Schema Namensraum für Namen, die in XML Dokumenten verwendet werden können

5.3 PVP2 Attribute

5.3.1 Syntaxangaben / Augmented BNF

Für Syntaxbeschreibungen wird die Augmented BNF wie in [RFC2616] verwendet. Sie wird um folgende Elemente ergänzt:

5.3.2 BNF Syntax

UACHAR = <druckbares US-ASCII (ISO-646) Zeichen ohne CRLF (dezimal 33-126)>
UTF_CHAR = <druckbares UNICODE Zeichen (nicht druckbar sind die Zeichen 0-31 und 127)>
SPACE = " "
SLASH = "/"
ALPHA = <Alle US-ASCII Buchstaben "A".."Z" und "a".."z">
DIGIT = <Ziffer zwischen 0 und 9>
NAMECHAR = ALPHA | DIGIT | "-" | "_"

5.3.3 Abbildung von PVP2 zu PVP1

Attributnamen

PVP2 hat vereinheitlichte Namen ohne hierarchische Organisation. Die Abbildung dieser unter "HTTP Header Name / SAML Attribute Name" bei jedem Attribut bezeichneten Namen wird auf die unter "PVP 1.x http Header Name" bzw. "PVP 1.9 XPATH-SOAP" angegebenen Namen abgebildet.

Feldlängen

PVP2 erlaubt bei einigen Attributen längere Werte, z.B. kann ein Name 128 statt 64 Zeichen lang sein. Bei einer Konvertierung nach PVP1 sind überlange Werte abzuschneiden.

Nicht mehr vorhandene Attribute

Authenticate-gvOuDomain, authorize-gvOuId /-Ou/-gvOuOkz haben keine Entsprechung in PVP 2 und sind bei der Konvertierung zu verwerfen.
Die Attribute TXID und zur Beschreibung des URL vor dem Umschreiben durch den Reverse Proxy werden nur im R-Profil geführt.

Geänderte Pflichtfelder

SecClass ist in PVP2 verpflichtend. Sollte die SecClass bei einer Konvertierung von PVP1 nach PVP2 fehlen, ist der Wert 1 einzusetzen.
-INVOICE-RECPT-ID/-COST-CENTER-ID/-CHARGE-CODE mussten in PVP1 als Tripel gemeinsam oder gar nicht angegeben werden. Zur Vereinfachung von PVP2 kann jedes Attribut für sich angegeben werden.

5.3.4 OIDs für Attribute der PVP Spezifikation

Wo möglich werden etablierte LDAP Attributdefinition wiederverwendet.
Basis OID für in diesem Dokument definierte Attribute ist 1.2.40.0.10.2.1.1.261

5.3.5 Listenattribute

Die meisten PVP Attribute, deren Definition im Rahmen der allgemein gültigen LDAP-RFC's erfolgt sind als Multi-Value-Attribute definiert. (können mehrfach vorkommen / Reihenfolge darf nicht semantisch interpretiert werden – z.B. uid).

Aufgrund diverser technischer Probleme mit real existierenden Softwareimplementierungen SOLL in PVP auch bei Listen-Attributen (multi value attributes) nur ein Wert übermittelt werden. Software SOLL aber so implementiert werden, dass Anfragen auch dann verarbeitet werden können, wenn eine unsortierte Menge von Werten für ein Attribut angegeben ist.

5.3.6 Attributverzeichnis

5.3.6.1 Technische Informationen

PVP-eGovTokenVersion

OID

1.2.40.0.10.2.1.1.261.10

definiert durch PVP (dieses Dokument)

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.261.10

HTTP Header Name

X-PVP-EGOVTOKEN-VERSION

Bedeutung

Kennzeichnung der Version des Portalverbundprotokolls, der dem Attributprofil der Anfrage folgt. Es dürfen nur die in Folge aufgelisteten Werte verwendet werden.

(z.B. ist es nicht zulässig den Wert 1.8.9 zu verwenden, obwohl es eine PVP Spezifikation mit der entsprechenden Versionsnummer gab.)

Zukünftige Versionen von PVP können neue Werte einführen.

Mögliche Werte

Wert	Bedeutung
1.0	PVP 1.4 (BMI Gateway Protokoll)
1.1	PVP 1.5.3
1.2	PVP 1.6, PVP 1.7
1.8	PVP 1.8.x
1.9	PVP 1.9.x

XML-Schema-Type

xs:string

Länge: 4

Pflichtattribut: Ja

PVP 1.x http Header Name

X-VERSION

PVP 1.x XPATH-SOAP

/pvpToken[@version]

5.3.6.2 Namen

principal Name

OID

1.2.40.0.10.2.1.1.261.20

definiert durch PVP (dieses Dokument)

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.261.20

HTTP Header Name

X-PVP-PRINCIPAL-NAME

Bedeutung

Natürliche Personen: Nachname bzw. Familienname

Organisationen³: Organisationsbezeichnung

System Principals: Bezeichnung des Device/Service/Netzwerks (siehe auch [LDAP.gv.at-PV] gvSystem/cn).

Syntax:

pn-value = 1#128 UTF_CHAR

XML-Schema-Type

xs:string

Länge: 128**Pflichtattribut: Ja****PVP 1.x http Header Name / PVP 1.x XPATH-SOAP**

Folgende Bildungsregel ergibt das PVP1-Header-Attribut cn aus den PVP2-Headern principalName und givenName:

$$cn = X-PVP-PRINCIPAL-NAME [+ SPACE + SPACE + givenName]^4$$

³ Für Österreich ist es nicht vorgesehen dass Organisationen sich als Principals anmelden; in anderen EU-Ländern ist das aber möglich.

⁴ Das doppelte Leerzeichen dient zur besseren Konvertierung der Datenstruktur von v2.0 -> v1.9 -> v2.0, damit Nachnamen mit Leerzeichen korrekt konvertiert werden.

Vorname (givenName)

OID

2.5.4.42; definiert in RFC 4519

SAML Attribute Name

urn:oid: 2.5.4.42

PVP-HTTP Header Name

X-PVP-GIVEN-NAME

Definition gem. RFC 4519

The 'givenName' attribute type contains name strings that are the part of a person's name that is not their surname. Each string is one value of this multi-valued attribute.

(Source: X.520 [X.520])

(2.5.4.42 NAME 'givenName'
SUP name)

Examples: "Andrew", "Charles", and "Joanne".

Anmerkung

Nur wenn eine natürliche Personen (und nicht eine Serveranwendung) den Zugriff tätigt.

Anders als im RFC Beispiel sollen Personen mit mehreren Vornamen durch Leerzeichen getrennt in einem Wert übertagen werden. (Abgesehen von allgemeinen technischen Schwierigkeiten mit Multi-Value-Attributen, kann nur so kann die Reihenfolge der Vornamen abgebildet werden)

Syntax:

gn-value = 1#128 UTF_CHAR

XML-Schema-Type

xs:string

Länge: 128

Pflichtattribut: Nein

PVP 1.x http Header Name / PVP 1.x XPATH-SOAP

Abbildung auf cn: siehe 0

5.3.6.3 Identifikationskennzeichen

Benutzerkennung (userId)

OID

2.5.4.42; definiert durch RFC 4519

SAML Attribute Name

urn:oid: 2.5.4.42

HTTP Header Name

X-PVP-USERID

Bedeutung gem RFC 4519

The 'uid' ('userid' in RFC 1274) attribute type contains computer system login names associated with the object. Each name is one value of this multi-valued attribute. (Source: RFC 2798 [RFC2798] and RFC 1274 [RFC1274])

```
( 0.9.2342.19200300.100.1.1 NAME 'uid'  
    EQUALITY caseIgnoreMatch  
    SUBSTR caseIgnoreSubstringsMatch  
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

1.3.6.1.4.1.1466.115.121.1.15 refers to the Directory String syntax [RFC4517].

Examples: "s9709015", "admin", and "Administrator".

XML-Schema-Type

xs:string

Pflichtattribut: Ja**PVP 1.x http Header Name**

X-AUTHENTICATE-USERID

PVP 1.9 XPATH-SOAP

authenticate/*Principal/UserID

Globale Account Kennung (gid)

OID

1.2.40.0.10.2.1.1.1

Definiert durch ldap.gv.at

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.1

HTTP Header Name / SAML Attribute Name

X-PVP-GID

Bedeutung gem. ldap.gv.at

Global eindeutiger Identifier bestehend aus: ‚AT:‘, einem Präfix, der die Systematik (z.b. personalführende Organisation, IT-System,...) bezeichnet, sowie einem zumindest innerhalb der Systematik unverwechselbar einer Person zuordenbarem Identifier.

(AT:BPK:ZP:j/NxdRQhp+tNyE9WhHdBSYuy3hA=

AT:B:0:123456 PMSAP-Nr.im Bundesbereich,

AT:L6:12345 im Länderbereich,

AT:GGA-31001:1234 im Gemeindebereich)

Anmerkung: Stabiler Identifier für einen IdP Account. Wird von Anwendungen verwendet, um Benutzende wiederzuerkennen.

XML-Schema-Type

xs:string

Maximallänge: 128**Pflichtattribut: Ja****PVP 1.x http Header Name**

X-AUTHENTICATE-GVGID

PVP 1.9 XPATH-SOAP

authenticate/*Principal/gvGid

Bereichsspezifische Personenkennung (gvpBK)

OID

1.2.40.0.10.2.1.1.149

Definiert durch ldap.gv.at

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.149

HTTP Header Name

X-PVP-BPK

Bedeutung

Bereichsspezifisches Personenkennzeichen inklusive Bereichsangabe.
Im Portalverbund der österreichischen Behörden wird die BPK für den Bereich Personalverwaltung (Bereichskürzel PV) im gesamten Verbund verwendet.

Beispiele:

PV:j/NxdRQhp+tNyE9WhHdBSYuy3hA=

XML-Schema-Type

xs:string

Pflichtattribut: Nein**PVP 1.x http Header Name**

X-AUTHENTICATE-GVPBK

PVP 1.9 XPATH-SOAP

authenticate/userPrincipal/gvBpk

5.3.6.4 Organisatorische Zugehörigkeiten

siehe auch 5.3.6.9

Kennung des Verbundteilnehmers (participantId)

OID

1.2.40.0.10.2.1.1.71

Definiert durch ldap.gv.at-PV

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.71

HTTP Header Name

X-PVP-PARTICIPANT-ID

Anmerkung

gvOuid (siehe 0) der Verbund-Teilnehmer für die eine Anfrage gestellt wurde. Basierend auf der ParticipantId kann für den SP festgelegt werden, welche Ressourcen für die Teilnehmer freigeschalten werden und welche nicht.

XML-Schema-Type

xs:string

Pflichtattribut: Ja**PVP 1.x http Header Name**

X-AUTHENTICATE-PARTICIPANTID

PVP 1.9 XPATH-SOAP

authenticate/participantId

Organisationskennzeichen der Organisationseinheit (ouOKZ)

OID

1.2.40.0.10.2.1.1.153

Definiert durch ldap.gv.at

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.153

HTTP Header Name

X-PVP-OU-OKZ

Bedeutung gem. ldap.gv.at

Eindeutiges alphanumerisches Kennzeichen für Organisationseinheit, externes Verwaltungskennzeichen (AT + VKZ) nach [VKZ] (AT:BMI-S1-3); cis(32), Single-Value

Anmerkung

Die Spezifikation Verwaltungskennzeichen ([VKZ]) definiert jetzt auch den Begriff OKZ, um auch Organisationen des Privatrechtes abbilden zu können.

Als PVP Attribute soll das OKZ 0 EINER Organisationseinheit für die der Benutzer tätig ist (Stammdienststelle), übermittelt werden. Bestehen

Bauftragungsverhältnisse zu mehreren Organisationseinheiten so MUSS der IdP die Möglichkeit anbieten eine der zugeordneten Einheiten auszuwählen.

Service Provider DÜRFEN Zuordnungen von Organisationseinheiten NICHT nutzen, um daraus Anwendungsrechte abzuleiten. Der Vertragspartner eines Service

Providers ist der Participant. Diesem wird die Möglichkeit eingeräumt frei zu

entscheiden, welche seiner Mitarbeiter welche Aufgabe erledigen sollen. Abgesehen davon entstünde sonst die Problematik, dass Organisationen eine interne

Umstrukturierung mit allen externen Service-Providern koordinieren müssten.

Syntax:

gvOuOKZ-value = 1#35 UACHAR

(die in ldap.gv.at genannte Maximal-Länge von 32 ist falsch, da die ouOKZ aus „AT:“ und einem max. 32 Zeichen langen OKZ besteht)

XML-Schema-Type

xs:string

Pflichtattribut: Nein

PVP 1.9.2 http Header Name

Ab PVP 1.9.2 wird diese Information mit dem optionalen Header X-AUTHENTICATE-GVOUOKZ übertragen:

gvOuid der Organisationseinheit (ouGvOuid)

OID

1.2.40.0.10.2.1.1.3

Definiert durch ldap.gv.at

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.3

HTTP Header Name / SAML Attribute Name

X-PVP-OU-GV-OU-ID

Bedeutung gem. ldap.gv.at

Primärschlüssel für Organisationseinheit

Syntax:

gvOuid ::= Landeskennung ":" ID

ID ::= "VKZ:" VKZ | Org-Id

VKZ... Verwaltungskennzeichen gem [VKZ]

Org-Id... Org-Id gem [VKZ]

Landeskennung...gem ISO 3166 - Alpha2

(AT:VKZ:GGA1234, AT:L9:9876)

Anmerkung

gvOuid ((wie [ldapgvat] gvOrgUnit / gvOuid; siehe auch 0) der Organisationseinheit, die auch mit „0 Organisationskennzeichen der Organisationseinheit (ouOKZ)“ beschrieben wird.

Syntax:

ouGvOuid-value = 1#39 UACHAR

Die in ldap.gv.at genannte Maximallänge ist falsch, da eine gvOuid auf „AT:VKZ:“ und einem bis zu 32 Zeichen langem OKZ bestehen kann

XML-Schema-Type

xs:string

Pflichtattribut: Ja**PVP 1.x http Header Name**

X-AUTHENTICATE-GVUID

Kurzbezeichnung der Organisationseinheit (ou)

OID

2.5.4.11

Definiert durch Annex A of Rec. ITU-T X.520 (February 2001) und ISO/IEC 9594-6: 2001: "The Directory: Selected attribute types" (Quelle: www.oid-info.com)

SAML Attribute Name

urn:oid:2.5.4.11

HTTP Header Name /

X-PVP-OU

Anmerkung

Kurzbezeichnung der mit ouGvOuid und ouOKZ referenzierten Organisationseinheit

Maximale Länge:

64

Syntax:

ou-value = 1#64 UTF_CHAR

XML-Schema-Type

xs:string

Pflichtattribut: Ja**PVP 1.x http Header Name außer 1.8**

X-AUTHENTICATE-OU

PVP 1.8

-

PVP 1.9 XPATH-SOAP

authenticate/*Principal/ou

Funktionsbezeichnung (function)

OID

1.2.40.0.10.2.1.1.33

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.33

HTTP Header Name

X-PVP-FUNCTION

Anmerkung

Bezeichnung der Funktion der Benutzer.

IdP können zu Personen Funktionen definieren und PVP Rollen den Funktionen einer Person zuordnen. (siehe ldap.gv.at gvOrgPerson / gvPersonFunction). Personen mit mehreren Funktionen muss dann am IDP eine Funktion zur Verfügung gestellt werden, mit der festgelegt werden kann, in welcher Funktion sie aktuell tätig sind. Werden Rechte Funktionen einer Person zugeordnet, so ist die Bezeichnung der Funktion, aus der die gemeldeten Zugriffsrechte abgeleitet wurden, als PVP Attribut anzugeben.

Funktion dieses Attributes ist die Nachvollziehbarkeit der einem Zugriff zugrunde liegenden Rechtezuordnungsprozesse zu vereinfachen.

Syntax:

function-value = 1#32 UTF_CHAR

XML-Schema-Type

xs:string

Länge: 32**Pflichtattribut: Nein****PVP 1.x http Header Name**

X-AUTHENTICATE-GVFUNCTION

PVP 1.9 XPATH-SOAP

authenticate/userPrincipal/gvFunction

5.3.6.5 Kontaktinformationen

E-Mail Adresse (mail)

OID

0.9.2342.19200300.100.1.3

Definiert durch RFC 4524

SAML Attribute Name

Urn:oid:0.9.2342.19200300.100.1.3

HTTP Header Name / SAML Attribute Name

X-PVP-MAIL

Anmerkung

E-Mail Adresse im einfachen Format gemäß der <Mailbox>
Produktionsregel aus RFC822 (localpart@domain; ohne Display-Namen)

z.B.

Maria.Muster@musterland.gv.at

XML-Schema-Type

xs:string

Länge: 128

Pflichtattribut: Nein

PVP 1.x http Header Name

X-AUTHENTICATE-MAIL

PVP 1.9 XPATH-SOAP

authenticate/userPrincipal/mail

Telefonnummer (tel)

OID

2.5.4.20

Definiert durch Annex A of Rec. ITU-T X.520 (February 2001) und ISO/IEC 9594-6: 2001: "The Directory: Selected attribute types" (Quelle: www.oid-info.com); wird von RFC 2798 (Definition inetOrgPerson) verwendet

SAML Attribute Name

urn:oid:2.5.4.20

HTTP Header Name

X-PVP-TEL

Anmerkung

Telefonnummer im internationalen Format gem. ITU-T E.123; führendes „+“ danach nur Ziffern und optionale Leerzeichen (nach dem Landescode und nach der Netzwahl))

Beispiele:

+43 1 4000

+351 213 927860

+43 680 3193140

+43 4823 2244

XML-Schema-Type

xs:string

Maximallänge: 32

Pflichtattribut: Nein

PVP 1.x http Header Name

X-AUTHENTICATE-TEL

PVP 1.9 XPATH-SOAP

authenticate/userPrincipal/te1

5.3.6.6 Sicherheitsklasse des Principals

Im S-Profil wird dieses Attribut nicht als Teil des PVPeGovTokens definiert, sondern wie in [SAML2IAProf] spezifiziert als SAML AuthenticationContext übermittelt.

PVP-eGovTokenVersion

HTTP Header Name

X-PVP-SECCLASS

Bedeutung

Sicherheitsklasse des Principals laut [SecClass].

Mögliche Werte

Laut [SecClass].

XML-Schema-Type

xs:integer

Länge: 1

Pflichtattribut: Ja

PVP 1.x http Header Name

X-AUTHENTICATE-gvSecClass

PVP 1.x XPATH-SOAP

authenticate/*Principal/gvSecClass

5.3.6.7 Berechtigungen / Autorisierung / Rollen

Roles (roles)

OID

1.2.40.0.10.2.1.1.261.30

Definiert durch PVP (dieses Dokument)

SAML Attribute Name

Urn:oid:1.2.40.0.10.2.1.1.261.30

HTTP Header Name / SAML Attribute Name

X-PVP-ROLES

Bedeutung

Beschreibt die Rechte /Rollen, die den Benutzern von der zuständigen vom Participant beauftragen Rechteverwaltung zugeordnet wurden.

Die möglichen Rollen einer Anwendung werden durch gvApplicationRight Objekte beschrieben.

Vorgaben, Anleitung und Tipps zur Modellierung von PVP Rechtesystemen sind der Konvention „Rechtemodellierung für Portalverbundanwendungen“

[AG_IZ_Rechtemodell] zu entnehmen. Für neue Anwendungen im Portalverbund der österreichischen Behörden ist die Einhaltung der Konvention verpflichtend.

Syntax (Argmented BNF wie in RFC2616)

Roles = Role *(,,"Role) [;]

Role = RoleName [,(, [Parameters] ")"]

Parameters = Parameter [,, " Parameter]

Parameter = ParameterName "=" ParameterValue

RoleName = 1#NameChar

ParameterName = 1#NameChar

ParameterValue = 1#UTF_CHAR

Kodierungsregeln für Parameterwerte

Folgende (syntaxrelevanten) Zeichen müssen in Parameterwerten kodiert werden, indem ein Backslash (\) vorangestellt wird:

Zeichen	Kodierung	Beschreibung
,	\,	Comma
)	\)	Closing bracket
\	\\	Backslash

Beispiel

APP_ABFRAGE(GKZ=10000, GKZ=20000);APP_UPDATE(GKZ=50000)

Länge:

32767

(Im Portalverbund der österreichischen Behörden gelten darüber hinaus die Maximallängenvorgaben aus der Konvention Rechtemodellierung¹³)

Pflichtattribut: Nein

XML-Schema-Type

xs:string

PVP 1.x http Header Name

X-AUTHORIZE-ROLES

PVP 1.9 XPATH-SOAP

authorize/role

5.3.6.8 Verrechnungsrelevante Informationen

Rechnungsempfänger (invoiceRecptId)

OID

1.2.40.0.10.2.1.1.261.40

Definiert durch PVP (dieses Dokument)

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.261.40

HTTP Header Name

X-PVP-INVOICE-RECPT-ID

Bedeutung

gvOuid (siehe 0) des Rechnungsempfängers.

Syntax

invoiceRecptId-value = 1#64 UACHAR

Länge: 64

Pflichtattribut: Nein

XML-Schema-Type

xs:string

PVP 1.x http Header Name

X-ACCOUNTING-INVOICERECPTID

PVP 1.9 XPATH-SOAP

accounting/InvoiceRecptId

Kostenstellen (costCenterId)**OID**

1.2.40.0.10.2.1.1.261.50

Definiert durch PVP (dieses Dokument)

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.261.50

HTTP Header Name

X-PVP-COST-CENTER-ID

Bedeutung

Liste der für Benutzer vorgegebenen Kostenstellencodes bzw. Angabe, dass bei kostenpflichtigen Transaktionen ein Eingabefeld angeboten werden muss, in dem frei eine beliebige Kostenstellenbezeichnung gewählt werden kann.

Werden Kostenstellen angegeben, so müssen Rechnungen des SP nach Kostenstellen gruppiert werden.

Stehen bei einer kostenpflichtigen Transaktion mehrere Kostenstellen zur Auswahl, so muss vom Service Provider eine Auswahl angeboten werden mit der festgelegt wird, an welche Kostenstelle diese Transaktion verrechnet werden soll.

Beispiele:`<default>ABC123,DEF456`

Benutzer haben die Kostenstellen ABC123 und DEF456 zur Auswahl, wobei ABC123 der Vorgabewert ist.

ABC123

Benutzer haben die Kostenstelle ABC123 fix vorgegeben.

`<default>ABC123, DEF456,<user defined>`

Benutzer haben die Kostenstellen ABC123 und DEF456 zur Auswahl, wobei ABC123 der Defaultwert ist. Außerdem können weitere Kostenstellen frei eingeben werden.

Syntax:`costCenterId-value = costCenterId-list | "<user defined>"``costCenterId-list = ["<default>"] costCenterId *["," costCenterId] [",<user defined>"]``costCenterId = 1#25 (NAMECHAR | SPACE | SLASH)`**XML-Schema-Type**

xs:string

Länge: 32767**Pflichtattribut:** Nein**PVP 1.x http Header Name**

X-ACCOUNTING-COSTCENTERID

PVP 1.9 XPATH-SOAP
accounting/CostCenterId

Gebührenstufe (chargeCode)**OID**

1.2.40.0.10.2.1.1.261.60

Definiert durch PVP (dieses Dokument)

SAML Attribute Name

urn:oid:1.2.40.0.10.2.1.1.261.60

http Header Name / SAML Attribute Name

X-PVP-CHARGE-CODE

Bedeutung

Liste der für Benutzer vorgegebenen Gebührenstufen (Codes für Transaktionsgebühr).

Sind bei einer (potentiell) kostenpflichtigen Transaktion mehrere Gebührenstufen möglich, so muss vom SP eine Möglichkeit geboten werden, die für die konkrete Transaktion zutreffende Stufe zu wählen.

Die Gebührenstufe "0" steht für gebührenfrei. Weitere Gebührenstufen können von Service-Providern beliebig definiert werden.

Ist eine Gebührenstufe angegeben, darf nur nach den angegebenen Gebührenstufen verrechnet werden.

Beispiele:

1

Die Gebührenstufe für die Anwendung ist fix vorgegeben

```
<default>0,1
```

Benutzer können sowohl gebührenfreie als auch Transaktionen der Gebührenstufe 1 nutzen. Können für eine Transaktion beide Gebührenstufen zur Anwendung gebracht werden, so ist eine Auswahl anzuzeigen in der Gebührenstufe 0 vorausgewählt ist.

0

Benutzer dürfen nur kostenfreie Transaktionen nutzen.

Syntax:

```
chargeCode-value = ["<default>"] chargeCode *["," chargeCode]  
chargeCode = 1#2 DIGIT
```

XML-Schema-Type

xs:string

Länge: 2**Pflichtattribut: Nein**

PVP 1.x http Header Name

X-ACCOUNTING-CHARGECODE

PVP 1.9 XPATH-SOAP

accounting/ChargeCode

*5.3.6.9 Reverse-Proxy Profil spezifische Parameter*Transaktionskennung (txid)**http Header Name / SAML Attribute Name**

X-PVP-TXID

Bedeutung

Um eine einheitliche Kennzeichnung von Log- und Protokoll-Einträgen bei IdP, SP und den Anwendungen zu ermöglichen, SOLL in Reverse Proxy Profilen der IdP bei jeder Anfrage eine für den ganzen Verbund eindeutige ID vergeben. Service Provider SOLLEN diese ID an die Zielanwendung weitergeben und für Protokollierung und Logging verwenden.

Syntax und Länge:

txid-value = uniqueID "@" domain
uniqueID = timestamp "\$" uniquenessString
timestamp = hours minutes seconds; Systemzeit in UTC (Universal Time Zone, Greenwich-Time, Zulu-Timezone)
hours = DIGIT DIGIT
minutes = DIGIT DIGIT
seconds = DIGIT DIGIT
uniquenessString 1#128 UACHAR

Länge: 128

Die TransaktionsID SOLL kürzer als 40 Zeichen sein, um die Lesbarkeit von Logfiles zu fördern.

Pflichtattribut: Nein**PVP 1.9 http Header Name (vor 1.9 war der Header nicht definiert)**

X-PVP-TXID

PVP 1.9 XPATH-SOAP

pvpExtension/debug-ticket/txid

URL der Transaktion wie vom Client benutzt: Schema**http Header Name**

X-PVP-ORIG-SCHEME

Bedeutung

Protokollschema (http oder https)

Syntax

1#8 UACHAR

Länge: 8

Pflichtattribut: Nein

PVP 1.9 http Header Name (vor 1.9 war der Header nicht definiert)

X-ORIG-SCHEME

PVP 1.9 XPATH-SOAP

pvpExtension/orig-host/scheme

URL der Transaktion wie vom Client benutzt: Host

http Header Name

X-PVP-ORIG-HOST

Bedeutung

FQHN inklusive :port, wenn nicht der Default port verwendet wird. RFC 2109: Fully-qualified host name means either the fully-qualified domain name (FQDN) of a host (i.e., a completely specified domain name ending in a top-level domain such as .com or .uk), or the numeric Internet Protocol (IP) address of a host. The fully qualified domain name is preferred; use of numeric IP addresses is strongly discouraged.

Syntax

1#256 UACHAR

Länge: 256

Pflichtattribut: Nein

PVP 1.9 http Header Name (vor 1.9 war der Header nicht definiert)

X-ORIG-HOST

PVP 1.9 XPATH-SOAP

pvpExtension/orig-host/host

URL der Transaktion wie vom Client benutzt: URI

http Header Name

X-PVP-ORIG-URI

Bedeutung

Pfadteil des URL mit führenden "/" und ohne Query Parameter.

Syntax

1#2048 UACHAR

Länge: 2048

Pflichtattribut: Nein

PVP 1.9 http Header Name (vor 1.9 war der Header nicht definiert)

X-ORIG-URI

PVP 1.9 XPATH-SOAP

pvpExtension/orig-host/uri

5.3.7 Application Chaining

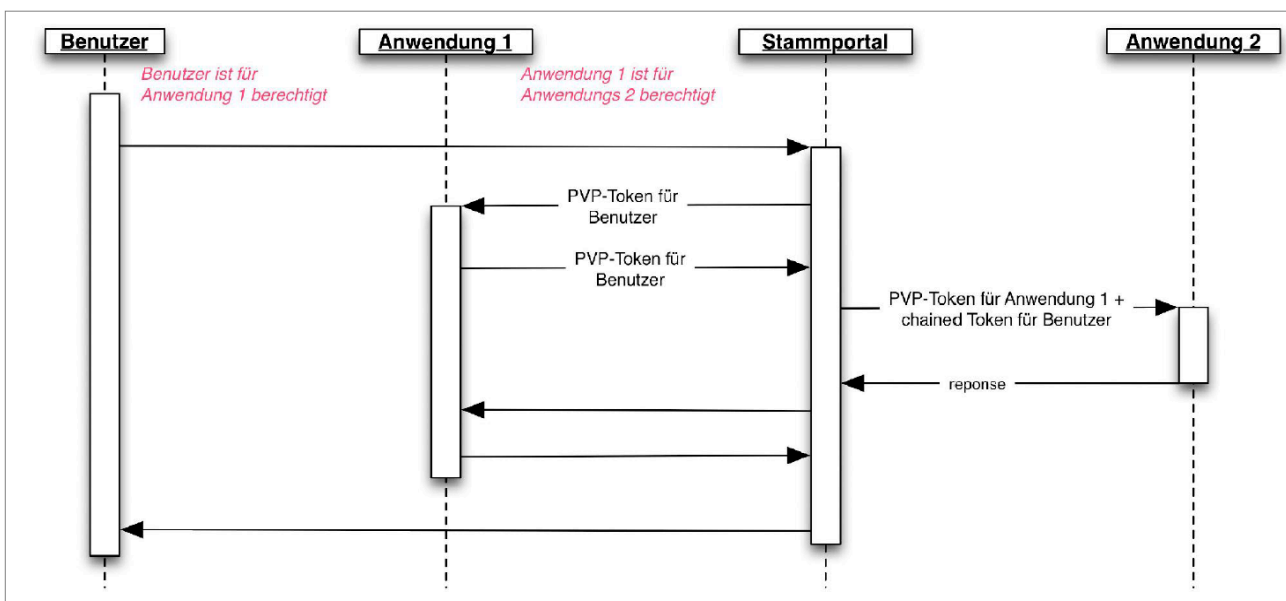
5.3.7.1 Allgemeines / Chained-Token

Welche Person für Zugriffe auf datenschutzrechtlich geschützte Inhalte verantwortlich ist, muss über Protokolle nachvollziehbar sein.

Wird auf ein Service der Föderation nicht über ein Endbenutzerdevice (z.B. Browser bei Zugriff auf eine Webanwendung) zugegriffen, sondern von einem Server-System aus (z.B. Webservice-Zugriff auf ein Register durch eine Web-Anwendung), müssen die PVP Zugriffsinformationen aller Vorläufer-Anfragen - einschließlich Endbenutzer - an das Zielservice gemeldet werden. (Chained-Token)

Das Chained-Token dient der Protokollierung bzw. wird dort verwendet, wo die Identität der Endanwender entscheidend ist (z.B.: Wird in einem Datenbestand die Kennung der Person, welche die letzte Änderung vorgenommen hat, vermerkt, muss dafür die Benutzerkennung der Endanwender verwendet werden, und nicht die eines zwischengeschalteten Systems).

Beispiel:



Benutzer greift über Stammportal auf Anwendung-1 zu. Das Stammportal meldet Anwendung-1 die PVP-Informationen der Endanwenderin. Bei der Anmeldung von Anwendung-1 am Stammportal für den Zugriff auf Anwendung-2 wird der PVP-Token dem Endanwender mitgeschickt. Nach erfolgreicher Anmeldung erzeugt der IDP(Stammportal) einen PVP-Token, für Anwendung-1. (Benutzer ist die Anwendung – es gelten auch die Rechte von Anwendung-1 an der Zielanwendung und nicht eventuelle Rechte der Endbenutzer). Die PVP-Informationen die die Anfragekette bis zur Endbenutzerin beschreiben werden als Chained-Token zusätzlich mitgeschickt.

5.3.7.2 Chained Token in SAML Profilen

Wie der Chained Token als SAML Attribute transportiert werden soll, ist bislang noch nicht definiert

5.3.7.3 Attribute des Chained-Tokens

Das Chained-Token beschreibt die Identität des zugreifenden Benutzers, und der Organisation(-seinheit)en, die den Zugriff zu verantworten haben. Greift ein Server-System auf eine Verbund-Ressource zu, so müssen von allen IdP-Anmeldungen der Anfragekette zumindest folgende PVP-Attribute als Chained-Headers gemeldet werden, sofern vorhanden:

- X-PVP-PARTICIPANT-ID
- X-PVP-USERID
- X-PVP-GID
- X-PVP-PRINCIPAL-NAME
- X-PVP-GIVEN-NAME
- X-PVP-OU-OKZ
- X-PVP-ROLES
- X-PVP-INVOICE-RECPT-ID
- X-PVP-COST-CENTER-ID
- X-PVP-CHARGE-CODE

Das Attribut X-PVP-EGOVTOKEN-VERSION wird nicht im Chained Token mitgeführt, da die Chained Token die gleiche Version wie der äußere Token haben müssen.

5.3.8 Chained-Token-Num-ID

Die Chained-Token-Num-ID wird zur Bildung von Attribut-Namen von PVP-Headern des Chained-Tokens verwendet. Sie besteht aus zwei Ziffern.

Für alle Benutzer der Anfragekette wird - beginnend beim Endanwender - eine fortlaufende numerische Kennzeichnung erzeugt. Für den - den Prozess auslösenden Zugriff der natürlichen Person - wird die Kennung 01 verwendet.

Theoretisch ist die Anzahl der Systeme deren Identität und organisatorische Verantwortlichkeit in Chained-Headers genannt werden muss unbeschränkt. PVP 1.x hat die Maximalanzahl auf zwei beschränkt – und bislang hat diese Grenze auch noch keinerlei praktische Probleme verursacht. Mit PVP-2 sind bis zu 99 zwischengeschaltete Systeme möglich.

Beispiel:

Das Web-Service „Anwendung-2“ aus „5.3.7.1 Allgemeines“ benutzt zur Beantwortung einer Anfrage ein weiteres Web-Service (=Anwendung-3). Bei diesem Zugriff wird die Identität und die Rechte von Anwendung-2 in den primären PVP-Parametern an Anwendung-3 gemeldet. PVP-Informationen der EndanwenderIn werden mit Chained-Token-Num-ID 01 gekennzeichnet. Die PVP Informationen des Zugriffs von Anwendung-1 auf Anwendung-2 werden mit der 02 gekennzeichnet.

Attributnamen für den Chained Token im Reverse Proxy Profil Die Attribute des Chained-Tokens werden eigenen http Headern gemeldet. Für die Bildung der

Headernamen wird wieder die Chained-Token-Num-ID verwenden.

Name = PVP-http-Header-Name „_“ Chained-Token-Num-ID

Beispiel:

Verwendete http Header-Namen, wenn der Zugriff an Anwendung-3 mit dem Reverse-Proxy-Profil abgewickelt wird.

- X-PVP-PARTICIPANT-ID_01
- X-PVP-USERID_01
- X-PVP-GID_01
- X-PVP-PRINCIPAL-NAME_01
- X-PVP-GIVEN-NAME_01
- X-PVP-OU-OKZ_01
- X-PVP-ROLES_01
- X-PVP-PARTICIPANT-ID_02
- X-PVP-USERID_02
- X-PVP-GID_02
- X-PVP-PRINCIPAL-NAME_02
- X-PVP-GIVEN-NAME_02
- X-PVP-OU-OKZ_02
- X-PVP-ROLES_02

5.3.9 Exkurs: IDs für Organisationen und OE im österr. E-Government

Dieses Kapitel gibt einen Überblick über Organisationskennzeichen, die in den Spezifikationen [VKZ] und ldap.gv.at beschrieben werden.

Es ist nicht normativ.

5.3.9.1 Kennzeichen nach der Spezifikation VKZ

Für Organisationen und Organisationseinheiten der österreichischen Verwaltung wurden in der Spezifikation VKZ 1.2¹⁴ zwei Kennzeichen eingeführt.

- Das Verwaltungskennzeichen / Organisationskennzeichen (früher VKZ jetzt OKZ)
- Org-ID

Im OKZ ist Semantik enthalten.

Beispiel: Das OKZ des Justizministeriums lautet *BMJ*

Die Org-ID besteht aus einem Präfix, die den Herausgeber der Nummer kennzeichnet und einer semantikfreien fortlaufende Nummer.

Beispiel: ie Org-ID des Justizministeriums lautet *B:1*.

Das OKZ soll leicht memoriert werden können. Es ist vorgesehen, um auf Schriftstücken genannt zu werden, oder als Suchbegriff in EDV Anwendungen.

Die Org-Id ist als „interner Schlüssel“ entworfen worden, um auf technischer Ebene eine Organisation(seinheit) zur referenzieren.

Motivation für die Einführung von zwei Ordnungsbegriffen war die Tatsache, dass besonders. im Bundesbereich Organisationen oft umbenannt werden. Dabei kann es notwendig sein, das OKZ zu ändern. Mit der Org-ID sollte ein stabiler Schlüssel geschaffen werden.

5.3.9.2 Kennzeichen nach ldap.gv.at

Obwohl die Kennzeichen der VKZ Spezifikation für die Verwendung in ldap.gv.at und im Portalverbund der Behörden entwickelt wurden, wurden im Rahmen der Einführung von ldap.gv.at Sonderformen der Organisationskennzeichner geschaffen. In den PVP-Attributen werden ausschließlich die Organisationskennzeichen nach ldap.gv.at verwendet.

gvOuid

Beim Aufbau der ldap.gv.at Verzeichnisdienste wurde eine neue Kennzeichnung für Organisationen eingeführt

Syntax:

gvOuid ::= Landeskennung ":" ID

ID ::= "VKZ:" VKZ | Org-Id

VKZ... Verwaltungskennzeichen gem [VKZ]

Org-Id... Org-Id gem [VKZ]

Landeskennung...gem ISO 3166 - Alpha2

(AT:VKZ:GGA1234, AT:L9:9876)

In ldap.gv.at und im Portalverbund ersetzte die gvOuid die Org-ID lt. VKZ. Durch einen Präfix für die Landeskennung („AT:") ist sie auch international verwendbar. Organisationen mit stabilem VKZ (z.B. Landesorganisationen, Gemeinden) können das VKZ verwenden, um Ihre gvOuid zu bilden. Bundesorganisationen verwenden eine Org-Id um Ihre gvOuid zu bilden.

Beispiele:

Die gvOuid des Justizministeriums lautet „AT:B:1“

Die gvOuid der Gemeinde Naas lautet „AT:VKZ:GGA-61731“

gvOuidVKZ

Mit ldap.gv.at 2.3 wurde auch für das VKZ eine Form mit einem Landespräfix geschaffen – für das gvOrgUnit Attribut gvOuidVKZ.

Syntax:

gvOuidVKZ ::= „AT:" VKZ

Beispiele:

Das gvOuidVKZ des Justizministeriums lautet „AT:BMJ“

Das gvOuidVKZ der Gemeinde Naas lautet „AT: GGA-61731“

5.3.9.3 Zusammenfassung

Für Organisationen der Bundesverwaltung wird die gvOuid über einen eigenen Nummernkreis generiert. Diese werden über ein zentrales LDAP Verzeichnis gemeinsam mit dem VKZ publiziert (siehe auch Abgleich von Portalverzeichnissen über ldap.gv.at).

Für alle anderen Organisationen werden die beiden Organisationskennzeichen aus dem VKZ generiert.

Die Spezifikation VKZ-EB definiert Regeln, wie für Organisationen der österreichischen Verwaltung, für im österreichischen Firmenbuch eingetragene Unternehmen, österreichische Vereine und im österreichischen Ergänzungsregister für sonstige Betroffene eingetragene Organisationen Verwaltungskennzeichen gebildet werden können.

Für Organisationen anderer Länder (die nicht im österreichischen Ergänzungsregister eingetragen sind) sind derzeit noch keine Regeln für die Bildung eines VKZ definiert.

Anhang A Beispiele für Rechte und Rechteparameter

Durch die zweidimensionale Darstellung von Rechten können die meisten Berechtigungssysteme mit angemessenem Aufwand abgebildet werden. Rechte an Anwendungen sind hier im Allgemeinen bereits aggregierte Einzelrechte, die in der Literatur oft als Rollen bezeichnet werden.

Einfaches Berechtigungsschema

- Recht 1: Anwendungsadministrator
- Recht 2: Sachbearbeiter
- Recht 3: Abfrageberechtigter

Komplexeres Berechtigungsschema

- Recht 1: Anwendungsadministrator
- Recht 2: Sachbearbeiter (OE)
- Recht 3: Abfrageberechtigter

In diesem Fall dürfen Sachbearbeiter nur für bestimmte Organisationseinheiten Geschäftsfälle erledigen. Dafür wird eine Liste von OE übergeben, für die der Benutzer die Rechte hat.

Das Modell ist auch für andere Einschränkungen oder explizite Berechtigungen einer Rolle anwendbar, etwa nach geografischen Gesichtspunkten.

Anhang B Referenzen

- [AG-IZ Glossar] Hörbe: Identity Management Glossar der AG-IZ
<http://www.ref.gv.at> | [Portalverbund](#) | [Zwischenergebnisse](#) | [PV Allgemein](#)
- [AG_IZ_Rechtemodell]
Stradal, Freidl, Gritschenberger, Pichler, Reif: Rechtemodellierung für Portalverbundanwendungen
<http://www.ref.gv.at> -> [Portalverbund](#)
- [LDAP.gv.at]
Spitzenberger: Spezifikation LDAP-gv.at V. 2.4.0
<http://www.ref.gv.at> -> [Portalverbund](#)
- [LDAP.gv.at-PV]
Hahn u. andere: Spezifikation LDAP-gv.at für Portalverbund
<http://www.ref.gv.at> -> [Portalverbund](#)
- [PortalV-PKI]
<http://portal.bmi.gv.at/ref/> -> PKI
- [PV-DASI]
Connert: Datensicherheitsmaßnahmen für Webanwendungen
<http://reference.e-government.gv.at>
- [PV-Whitepaper]
Hörbe, Werzowa: Portal Verbund Whitepaper 2005-02-17
<http://reference.e-government.gv.at> -> [Portalverbund](#)
- [PVV 1.0]
Connert, Grandits, Kotschy, Posch, Siegl: Vereinbarung über die einzuhaltenden Rahmenbedingungen bei der Einrichtung und Benützung eines E-Government Portalverbundsystems (21.11.2002)
<http://reference.e-government.gv.at> – Empfehlungen
- [RFC2616]
R. Fielding & al.: Hypertext Transfer Protocol -- HTTP/1.1
<http://www.ietf.org/rfc/rfc2616.txt>
- [SAML2IAProf]
OASIS Committee Specification 01, SAML V2.0 Identity Assurance Profiles Version 1.0, November 2010.
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf>
- [SecClass]
Hörbe: Sicherheitsklassen im Portalverbund-System
<http://reference.e-government.gv.at> – Empfehlungen
- [VKZ]
Grandits: Verwaltungskennzeichen:
<http://reference.e-government.gv.at> Dokument VKZ 1.2.0