Portalverbundprotokoll Version 2 **eGovernment Attribute Profile**		**Konvention** **PVP 2.1.3** **Ergebnis der AG 20.10.2017**
Kurzbeschreibung	Dieses Dokument definiert die möglichen Attribute, die im Portalverbund zwischen Stammportalen / Identity-Providern (IdP) und Anwendungsportalen / Service-Providern (SP) ausgetauscht werden. Die Attribute beschreiben Identifikationsinformationen, die organisatorische Zugehörigkeit, aber auch Autorisierungsinformationen (PVP-Rechte, Vollmachten)	
Autor(en):	Peter Pichler (LFRZ)	Projektteam / Arbeitsgruppe
		AG Integration und Zugänge (AG-IZ) AG-Leitung: Ing. Dipl.-Ing.(FH) Hannes Wittmann, MSc (Mag. Wien) Stellvertretung: Dipl.-Ing. Dominik Klauser, BSc (BKA)
Beiträge von:	Rainer Hörbe, Thomas Lenz, Joachim Minichshofer, Bernd Zwattendorfer, Harald Stradal	

Version 2.1.3 :	Angenommen: -
Version 2.1.2 : 01.06.2015	Angenommen: -
Version 2.1.1 : **16.4.2015**	Angenommen: -
Version 2.1.0 : **14.10.2013**	Angenommen: **21.11.2013** **VSt-1712/488**
Version 2.0.0 : **31.8.2011**	Angenommen: **14.10.2011** **VST-1712/455**

Inhaltsverzeichnis

1 Allgemeines

Mit PVP-Attributen werden den Service-Provider (SP) in normierter Form Informationen über die angemeldeten Benutzer zur Verfügung gestellt. Das hier spezifizierte Datenmodell wird über die verschiedenen Profile einheitlich umgesetzt um Interoperabilität über Gateways zu gewährleisten.

Das PVP Protokoll entstand rund um Zugriffe von Personal der öffentlichen Verwaltung auf Verwaltungsanwendungen (G2G, Government To Government). Mit Version 2.1 wurden auch jene Attribute, die von Bürgerinnen und Bürgern unter der Nutzung der Bürgerkarte Verwendung finden, in die PVP-Spezifikation mit aufgenommen.

Das Unternehmensserviceportal orientiert sich für Anwendungen aus der Wirtschaft ebenfalls am Portalverbundprotokoll. Weitere „Verbünde“, wie der Kammerportalverbund, der Wirtschaftsportalverbund, etc. orientieren sich ebenfalls am Portalverbundprotokoll.

Die tatsächliche Strukturierung hängt vom jeweiligen PVP-Profil ab:

- S-Profil:, R-Profil-SOAP: Die PVP-Attribute werden als Attribute einer SAML 2.0 Assertion abgebildet
- R-Profil-HTTP: Die PVP-Attribute werden in Form von HTTP Headern übertragen

Das verwendete Profil 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.

1.1 X500 Attribute Profile / NameFormat für SAML-Attribute

Das PVP-2-Attribute-Profil basiert auf dem „SAML 2.0 X.500/LDAP Attribute Profile“. (*urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500*)

Als NameFormat für SAML-Attribute sieht das X500 Profil *urn:oasis:names:tc:SAML:2.0:attrname-format:uri* vor.

Das PVP-2-Attribute-Profil verweist wo möglich auf existierende LDAP Attributdefinitionen bzw. – wenn kein Attribut aus existierenden X500 Attribute Definitionen anwendbar ist - wird eine neue OID durch das PVP2 Attribute Profil festgelegt

1.2 Andere Attribute Profiles

Primäres Ziel des PVP2-Attribute-Profiles ist eine klare Definition für Attribute festzulegen. Die Namen für SAML-Attribute wurden auf Basis von OIDs festgelegt. Dadurch ist die Eindeutigkeit der SAML-Bezeichnungen von PVP-Attributen sichergestellt. Darum können PVP-Attribute mit SAML-Attributen aus anderen Profilen kombiniert werden.

1.3 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 [XML DSIG]
xenc:	http://www.w3.org/2001/04/xmlenc#	Namensraum der XML Encryption Syntax and Processing Specification [XML-ENC]
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
eidas:	http://eidas.europa.eu/saml-extensions	eIDAS SAML Attribute Profile Namensraum, siehe

1.4 Allgemeines zur Definition von Attributen

1.4.1 Syntaxangaben / Augmented BNF

Für Syntaxbeschreibungen wird die *Augmented BNF* - wie in [RFC822] definiert - verwendet. Sie wird um folgende Elemente ergänzt:

1.4.2 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| “-“ | “_”
B64CHAR = <Zeichen aus Base64-Alphabet laut RFC 2045 (A..Z, a..z, 0..9, +, /, =) oder Whitespace>

1.4.3 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” 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.

Reverse Proxy spezifische Attribute
Attribute, die nur im Zusammenhang mit dem R-Profil sinnvoll sind (TXID, X-PVP-ORIG…) wurden nur für Reverse-Proxy definiert (es wurde keine OID und kein SAML-Attribut-Name festgelegt)

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.

1.4.4 OIDs für Attribute der PVP-Spezifikation

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

1.4.5 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 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.

1.5 Klassifikation der Identifier-Attribute (Nicht normativ)

Folgende Tabelle beschreibt verschiedene Qualitäten der im PVP-Protokoll der verfügbaren Identifier-Attribute:

Table 1 Qualität von Identifier Attributen bezüglich ihrer Eigenschaften

Identifier	Eigenschaften								
	1 Unique	2 Permanent	3 kein recycling	4 Bereichsspezifisch	5 servicespezifisch	6 opaque	7 UI-geeignet	8 verfügbar	9 Eindeutig Rückführbar
Mail	x						x	+	
GID	x	x	x					++	
UserID	x						x		
bPK	x	x	x	x		x		+/-	x
Persistent NameID[1]	x		x		x	x		++	
Name+Geburtsdatum	(x)[2]						x	+	

Table 2 Spezifikation der Eigenschaften von Identifier Attributen

1	Eindeutig innerhalb eines Bereichs
2	Dauerhaft (unveränderbar für Lebensdauer der Entität und danach für die Archivierung)
3	Nicht wiederverwendbar (kann keiner anderen Entität zugewiesen werden)
4	Bereichspezifisch nach Bereichsabgrenzungsverordnung (gilt nur für ein Service oder ein Gruppe von Services, im Gegensatz zu einem globalen Identifier)
5	Service-spezifisch. Ist pro SP unterschiedlich
6	Nicht beschreibend. Enthält keine Teile, aus denen Eigenschaften des Subjekts preisgeben (etwa so wie das Geburtsdatum der SVNR)
7	UI-geeignet (kann von Benutzern leicht gelesen oder geschrieben werden)
8	Vollständigkeit, praktische Verwendung bei den Teilnehmern in +/-
9	Die natürliche Person muss global auf genau einen Identifier rückführbar sein.

[1] Siehe SAML Spezifikation
[2] Kollision möglich aber nicht sehr wahrscheinlich

2 Änderungen gegenüber vorhergehenden Versionen

2.1 Änderungen gegenüber dem PVP 1.9 PVP-Token

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

- Die Protokollversion bezieht sich nur mehr auf den *PVP eGovToken*
- Die Attribute haben keine Hierarchie mehr (AUTHENTICATE, AUTHORIZE, …)
- Aufnahme von Attributen, die für die Verwendung von PVP als Schnittstelle für eine Bürgerkartenauthentifizierung notwendig sind.
- 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 druckbaren Unicode. Im R-Profil müssen Nicht-ASCII Zeichen mit Nummerischen-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)
- Chained-Token: Bei der Bildung der Attribute-Namen für das Chained-Token wurde die laufende Nummer vorangestellt. Die Namen werden jetzt durch Anhängen der laufenden Nummer gebildet.
- Diverse Detailänderungen bei den Attributen.

2.2 Änderungen von PVP 2.0.0 auf PVP 2.1.0

Mit der Version 2.1 wurde folgende Änderungen umgesetzt (nicht normativ):

- Neue Attribute für die Anbindung der österreichischen Bürgerkarte und des Konzeptes Online-Vollmachten.
- Der HTTP-Name für das PVP Versions Attribut wurde von "X-PVP-EGOVTOKEN-VERSION" auf " "X-PVP-VERSION" umbenannt
- Für das ldap.gv.at Attribut gvOuVKZ war bis zur Version 2.5 auch ein Landesprefix ("AT:") vorgesehen. Dieser wurde mit Version ldap.gv.at 2.5 entfernt. Das entsprechend nicht normative Kapitel 6 (Exkurs: IDs für Organisationen und Organisationseinheiten im österr. E-Government) wurde entsprechend angepasst.
- Neues Attribut: X-PVP-PARTICIPANT-OKZ. Bisher wurde nur die gvOuId des Verbundteilnehmers an das Anwendungsportal kommuniziert. Zahlreiche Anwendungen benötigen aber das OKZ/VKZ. Auch die Best-Practice-Konvention Rollenmodellierung sieht vor, Organisationen als Rechteparameter in Form einer OKZ/VKZ zu übermitteln. Ein vollständiges Verzeichnis aller Organisationen, über das mit Hilfe einer gvOuId ein OKZ/VKZ bezogen werden kann, ist nicht in Sicht.
- Falsche OID für das Attribut UserId. Irrtümlicherweise wurde bei der Beschreibung von X-PVP-USER-ID die falsche OID (2.5.4.42 = Given Name) verwendet. Die richtige OID ist 0.9.2342.19200300.100.1.1.
- Neuer HTTP-Header X-PVP-BINDING zur Deklaration der vom Stammportal gesetzten Bindings.

2.3 Änderungen PVP 2.1.1

- Bildungsregel von CN war falsch angegeben (jetzt Vorname Nachname)
- Falscher Parametername für X-PVP-TXID für PVP 1.9 angegeben (bisher X-PVP-TXID richtig X-TXID)
- Syntax gvRoles hatte einen Fehler
- Ergänzung/Korrektur PVP 1.9 XPATH Angabe für authenticate/userPrincipal/gvGid, authenticate/*Principal/gvOuOKZ, authenticate/*Principal/gvOuId, pvpExtension/orig-host/hostinfo
- CHARGE-CODE / Aus der Beschreibung wurde der Satz " Ist eine Gebührenstufe angegeben, darf nur nach den angegebenen Gebührenstufen verrechnet werden." entfernt, weil er nicht der technischen Spezifikation dient.

2.4 Änderungen PVP 2.1.2

- Neues Attribut: MANDATE-TYPE-OID. Zusätzlich zur textuellen Beschreibung des ausgewählten Vollmachten-Profils steht mit diesem Attribut nun auch eine maschinell lesbare Beschreibung des Vollmachten-Profils in Form einer OID zur Verfügung.

- Ergänzung der möglichen Werte des Attribute MANDATE-PROF-REP-OID um ELGA Ombudsstellen OIDs

2.5 Änderungen PVP 2.1.3

- Neues Kapitel: Klassifikation von Identifier-Attributen
- Beschreibung gvGid aktualisiert (an LDAP.gv.at 2.5.1 angepasst)
- Neues Attribut: EID-CITIZEN-QAA-EIDAS-LEVEL
- Attribute SECCLASS für S-Profil aktiviert
- Attribute EID-STORK-TOKEN entfernt
- Attribute EID-CITIZEN-QAA-LEVEL als deprecated markiert
- Referenzen auf STORK entfernt oder durch Referenzen auf eIDAS ersetzt

3 Attributverzeichnis

3.1 Technische Informationen

3.1.1 **PVP-Version (PVP-VERSION)**	
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
Friendly Name	PVP-VERSION
HTTP Header Name	X-PVP-VERSION
Bedeutung	Kennzeichnung der Version des Portalverbundprotokolls, das dem Attribut Profile 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. **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 2.0 PVP 2.0.x 2.1 PVP 2.1.x
Syntax	version-value = 1#4 (DIGIT | ".")
Länge	Max. 4
Beispiel	2.1
XML-Schema-Type	*xs:string*
PVP 1.x HTTP Header	X-VERSION
PVP 1.x XPATH-SOAP	/pvpToken[@version]
PVP 2.0 Header-Name	X-PVP-EGOVTOKEN-VERSION

3.1.2 Sicherheitsklasse des Principals (SECCLASS)	
OID	1.2.40.0.10.2.1.1.261.110; definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid: 1.2.40.0.10.2.1.1.261.110
Friendly Name	SECCLASS
HTTP Header Name	X-PVP-SECCLASS
Bedeutung	Sicherheitsklasse des Principals laut [SecClass].
Anmerkung	Im S-Profil wird die Sicherheitsklasse der Anmeldung als SAML AuthenticationContext wie in [SAML2IAProf] übermittelt. Die Angabe der Sicherheitsklasse erfolgt im S-Profil nicht auf Basis von Integer-Werten, sondern auf Basis von URIs.
Mögliche Werte	Laut [SecClass].
XML-Schema-Type	*xs:integer*
Syntax	secclass-value = DIGIT
Länge	1
Beispiel	3
PVP 1.x HTTP Header	X-AUTHENTICATE-gvSecClass
PVP 1.x XPATH-SOAP	authenticate/*Principal/gvSecClass

3.2 Angaben zum Benutzer

3.2.1 Bezeichnung / Nachname (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
Friendly Name	PRINCIPAL-NAME
HTTP Header Name	X-PVP-PRINCIPAL-NAME
eIDAS SAML-Attribute	In eIDAS wird bei natürlichen Personen der Nachname mit dem Attribute http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName beschrieben. Systembenutzer sind in eIDAS nicht vorgesehen.
Bedeutung	Natürliche Personen: Nachname bzw. Familienname Organisationen3: Organisationsbezeichnung System Principals: Bezeichnung des Device/Service/Netzwerks (siehe auch [LDAP.gv.at-PV] gvSystem/cn). Typischerweise fordert eine natürliche Person Ressourcen im Portalverbund an. Es gibt aber auch Anwendungsfälle, in denen ein technisches System eine Anfrage in einem Verbund stellt (z.B. eine Webanwendung, die über Webservices Anfragen an ein fremdes System stellt). Das Attribute PRINCIPAL-NAME bildet beide Varianten ab.
Syntax	pn-value = 1#128 UTF_CHAR
Länge	Max. 128
Beispiel	Mustermann
XML-Schema-Type	xs:string
PVP 1.x HTTP Header / PVP 1.x XPATH-SOAP	Folgende Bildungsregel ergibt das PVP1-Header-Attribut cn aus den PVP2-Headern principalName und givenName: `cn = [GIVEN-NAME SPACE SPACE ] PRINCIPAL-NAME`[4]

3.2.2 Vorname (GIVEN-NAME)	
OID	2.5.4.42 (definiert in RFC 4519)
SAML-Attribute Name	urn:oid:2.5.4.42
Friendly Name	GIVEN-NAME
PVP-HTTP Header Name	X-PVP-GIVEN-NAME
eIDAS SAML-Attribute	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName
Bedeutung	Die Definition erfolgt gem. RFC 4519 [RFC4519] 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)

[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.

	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 die Reihenfolge der Vornamen abgebildet werden)
Syntax	gn-value = 1#128 UTF_CHAR
Länge	Max. 128
Beispiel	Max August
XML-Schema-Type	xs:string
PVP 1.x HTTP Header / PVP 1.x XPATH-SOAP	Abbildung auf cn: siehe 3.2.1 Bezeichnung/Nachname

3.2.3 Geburtsdatum (BIRTHDATE)

OID	1.2.40.0.10.2.1.1.55 (definiert durch ldap.gv.at)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.55
Friendly Name	BIRTHDATE
HTTP Header Name	X-PVP-BIRTHDATE
eIDAS SAML-Attribute	http://eidas.europa.eu/attributes/naturalperson/DateOfBirth
Bedeutung	(nicht normativ) Geburtsdatum im Format JJJJ-MM-TT Sind Monat und/oder Tag der Geburt nicht bekannt, wird der Wert „00“ verwendet.
Syntax	birthdate-value = 4#4 DIGIT “-“ 2#2 DIGIT “-“ 2#2 DIGIT
Länge	10
Beispiele	1972-02-13 1944-00-00
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	-
PVP 1.x XPATH-SOAP	-

3.2.4 Benutzerkennung (USERID)

OID	0.9.2342.19200300.100.1.1 (definiert durch RFC 4519 [RFC4519])
SAML-Attribute Name	urn:oid:0.9.2342.19200300.100.1.1
Friendly Name	USERID
HTTP Header Name	X-PVP-USERID
Bedeutung	Die Definition erfolgt gem. RFC 4519 [RFC4519]: 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] . Ldap.gv.at sieht vor, dass für Werte dieses Attributes das E-Mail-Adressen-Format gem. RFC 822 zu verwenden ist.
Syntax	userid-value = 1#128 NAMECHAR
Länge	Max. 128
Beispiel	Vorname.Nachname@org.gv.at user567@org.gv.at"
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-USERID
PVP 1.9 XPATH-SOAP	authenticate/*Principal/UserID

3.2.5 Globale Account Kennung (GID)

OID	1.2.40.0.10.2.1.1.1 (definiert durch ldap.gv.at [LDAP.gv.at]
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.1
Friendly Name	GID
HTTP Header Name / SAML-Attribute Name	X-PVP-GID
Bedeutung	Definition gem. ldap.gv.at: Global eindeutiger Identifier bestehend aus einem mit ‚AT' beginnenden Präfix: der den zentral erfassten Namespace (z.B. VKZ der personalführenden Organisation, IT-System,) im gesamten Verbund eindeutig bezeichnet, sowie einem innerhalb des Namespace unverwechselbar einer Person zuordenbarem nicht wiederverwendbaren Identifier.
Anmerkung	Stabiler Identifier für einen IdP Account. Wird von Anwendungen verwendet, um Benutzende wiederzuerkennen.
Syntax	gid-value = „AT:" 1#125 UTF_CHAR
Länge	Max. 128
Beispiele	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
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-GVGID
PVP 1.9 XPATH-SOAP	authenticate/userPrincipal/gvGid

3.2.6 Bereichsspezifisches Personenkennzeichen (BPK)

OID	1.2.40.0.10.2.1.1.149 (definiert durch ldap.gv.at [LDAP.gv.at])
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.149
Friendly Name	BPK
HTTP Header Name	X-PVP-BPK

Bedeutung	Bereichsspezifisches Personenkennzeichen (bPK) inklusive Bereichsangabe. Dabei kann es sich um ein bPK für den behördlichen als auch den privatwirtschaftlichen Bereich (wbPK) handeln. Für die Berechnung eines bPK wird im behördlichen Bereich das Bereichskürzel des jeweiligen staatliche Tätigkeitsbereichs gemäß Bereichsabgrenzungsverordnung [BerAbgrV] herangezogen. Im Portalverbund der österreichischen Behörden KANN die bPK für den Bereich Personalverwaltung (Bereichskürzel PV) für Personal des Bundes verwendet werden. Für die Berechnung eines bPK des privatwirtschaftlichen Bereichs (wbPK) wird die jeweilige Stammzahl des Auftraggebers (z.B. Firmenbuchnummer) herangezogen. Der Typ des übertragenen bPKs wird dabei über das Attribut „EID-SECTOR-FOR-IDENTIFIER“ (siehe Abschnitt 3.5.4) angegeben. Siehe [bPK-Algo].
Syntax	bPK-value := (BEREICH ":" bPK) BEREICH := 1#NAMECHAR (Verwaltungsbereich gem. Bereichsabgrenzungsverordnung bei Verwaltungsanwendungen bzw. Stammzahl des Auftraggebers bei Anwendungsverantwortlichen aus der Privatwirtschaft) bPK := 1# B64CHAR (bereichsspezifisches Personenkennung für den angegebenen Verwaltungsbereich bzw. Auftraggeber)
Länge	Max. 1024
Beispiele	PV:j/NxdRQhp+tNyE9WhHdBSYuy3hA= XFN+468924i: sJ0uDLw8UQNEbhChZpwKCPSSp9thLzKQI=
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-GVBPK
PVP 1.9 XPATH-SOAP	authenticate/userPrincipal/gvBpk

3.2.7 Verschlüsselte Bereichsspezifische Personenkennzeichen / Fremd-bPK (ENC-BPK-LIST)

OID	1.2.40.0.10.2.1.1.261.22 definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.22
Friendly Name	ENC-BPK-LIST
HTTP Header Name	X-PVP-ENC-BPK-LIST
Bedeutung	Liste von Fremd-bPK´s (=verschlüsselte bPK´s) der zugreifenden Person. Fremd-bPKs beziehen sich nur auf den behördlichen Bereich und NICHT für den privatwirtschaftlichen Bereich. Ob – und welche Fremd-bPK´s an eine Zielanwendung übermittelt werden – muss am IdP geregelt werden. Es muss im Rahmen der Einrichtung geprüft werden, ob die Berechnung und Übermittlung für die konkrete Anwendung notwendig und zulässig ist.
Syntax	EncSSPINList := EncSSPIN [";" EncSSPINList] EncSSPIN := "(" VKZ “+“ BEREICH “|“ FremdbPK ")" BEREICH := #2 ALPHA | (#2 ALPHA “-“ #2 ALPHA) VKZ := #32 NAMECHAR FremdbPK := 1#256 B64CHAR
Länge	Max. 32767
Beispiele	(BMI+T1|c1tWDIrXH3BQ95bUKNUXFaxKoY4o1t01n59XwE2WCgsSuj AEWslYQn5rEZVNfBkjjqdGI-cOORN2sbi8PSQS+3h131e7uO+U2KoXA/jN3VwESLA1I0sbabTUChY1n BzlublLrjCyI/sJ0uDLw8UQNEbhChZpwKCPSSp9thLzKQI=);(BMI+T2|P HdlaXRlcmUgRnJlbWQtYlBLKD12ZXJzY2hs/HNzZWx0ZSBi-UEsgKGdlaGFzaGVkLC-BrYW5uIG5pY2h0IGFscyBTY2hs/HNzZWwgdmVyd2VuZGV0IH-dlcmRlbikpPg==)
XML-Schema-Type	xs:string

PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.9 XPATH-SOAP	Nicht verfügbar

3.2.8 E-Mail Adresse (MAIL)

OID	0.9.2342.19200300.100.1.3 Definiert durch RFC 4524 [RFC4524]
SAML-Attribute Name	urn:oid:0.9.2342.19200300.100.1.3
Friendly Name	MAIL
HTTP Header Name	X-PVP-MAIL
Bedeutung	E-Mail Adresse im einfachen Format gemäß der <Mailbox> Produktionsregel aus RFC822 [RFC822] (localpart@domain; ohne Display-Namen)
Syntax:	<Mailbox> gem. RFC822
Länge	Max. 128
Beispiel	Maria.Muster@musterland.gv.at
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-MAIL
PVP 1.9 XPATH-SOAP	authenticate/userPrincipal/mail

3.2.9 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 [RFC2798] (Definition inetOrgPerson) verwendet
SAML-Attribute Name	urn:oid:2.5.4.20
Friendly Name	TEL
HTTP Header Name	X-PVP-TEL
Bedeutung	Telefonnummer im internationalen Format gem. ITU-T E.123; führendes „+“ danach nur Ziffern und optionale Leerzeichen (nach dem Landescode und nach der Netzvorwahl))
Syntax	tel-value := “+“ {1-31} (DIGIT | “ “)
Länge	Max. 32
Beispiele	+43 1 4000 +351 213 927860 +43 680 3193140 +43 4823 2244
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-TEL
PVP 1.9 XPATH-SOAP	authenticate/userPrincipal/tel

3.3 Organisatorische Zugehörigkeiten

(siehe auch Abschnitt 6 Exkurs: IDs für Organisationen und Organisationseinheiten im österr. E-Government)

3.3.1 gvOuId des Verbundteilnehmers (PARTICIPANT-ID)	
OID	1.2.40.0.10.2.1.1.71; definiert durch ldap.gv.at-PV [LDAP.gv.at-PV]
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.71
Friendly Name	PARTICIPANT-ID
HTTP Header Name	X-PVP-PARTICIPANT-ID
Bedeutung	gvOuId (siehe auch 6.2 gvOuId – Schlüssel für Organisationen nach ldap.gv.at) 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.
Syntax	gvOuID = Landeskennung ":" ID ID = "VKZ:" VKZ | Org-Id VKZ ::= 1#32UACHAR;(Verwaltungskennzeichen gem. [VKZ]) Org-Id ::= 1#32UACHAR;(Org-Id gem. [VKZ]) Landeskennung ::= {2} ALPHA; (gem. ISO 3166 - Alpha2) (nicht normativ / nach ldap.gv.at)
Länge	Max. 39; (Die in ldap.gv.at genannte Maximallänge ist falsch, da eine participant-Id aus „AT:VKZ:“ und einem bis zu 32 Zeichen langem OKZ bestehen kann)
Beispiele	"AT:B:102", "AT:VKZ:GGA-12345", "AT:L9:9876"
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-PARTICIPANTID
PVP 1.9 XPATH-SOAP	authenticate/participantId

3.3.2 OKZ/VKZ des Verbundteilnehmers (PARTICIPANT-OKZ)	
OID	1.2.40.0.10.2.1.1.261.24 (definiert durch PVP (dieses Dokument))
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.24
Friendly Name	PARTICIPANT-OKZ
HTTP Header Name	X-PVP-PARTICIPANT-OKZ
Bedeutung	OKZ/VKZ der durch 3.3.1 (gvOuId des Verbundteilnehmers (PARTICIPANT-ID)) bezeichneten Organisation.
Syntax	gvOuOKZ-value = {1-32} UACHAR
Länge	Max. 32
Beispiele	BMI GGA-12345 L9
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	-
PVP 1.9 XPATH-SOAP	-

3.3.3 Organisationskennzeichen der Organisationseinheit (OU-OKZ)	
OID	1.2.40.0.10.2.1.1.153; definiert durch ldap.gv.at [LDAP.gv.at]
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.153

HTTP Header Name	X-PVP-OU-OKZ
Friendly Name	OU-OKZ
Bedeutung	Definition gem. ldap.gv.at Eindeutiges alphanumerisches Kennzeichen für eine Organisationseinheit, externes Verwaltungskennzeichen nach [VKZ]
Anmerkung	Die Spezifikation Verwaltungskennzeichen ([VKZ]) definiert jetzt auch den Begriff OKZ, um auch Organisationen des Privatrechtes gerecht zu werden. Als PVP Attribut soll das OKZ EINER Organisationseinheit, für die der Benutzer tätig ist (Stamm-OE), übermittelt werden. Bestehen Beauftragungsverhältnisse zu mehreren Organisationseinheiten so MUSS der IdP die Möglichkeit anbieten, eine der zugeordneten Einheiten auszuwählen. Service-Provider (SP) 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.
Syntax / Länge / Beispiel / XML Schema-Type	siehe 3.3.2 OKZ/VKZ des Verbundteilnehmers (PARTICIPANT-OKZ)
PVP 1.9.2 HTTP Header Name	Ab PVP 1.9.2 wird diese Information mit dem optionalen Header X-AUTHENTICATE-GVOUOKZ übertragen.
PVP 1.9 XPATH-SOAP	authenticate/*Principal/gvOuOKZ

3.3.4 gvOuId der Organisationseinheit (OU-GV-OU-ID)

OID	1.2.40.0.10.2.1.1.3; definiert durch ldap.gv.at [LDAP.gv.at]
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.3
Friendly Name	OU-GV-OU-ID
HTTP Header Name	X-PVP-OU-GV-OU-ID
Bedeutung	Definition gem. ldap.gv.at:Primärschlüssel für Organisationseinheit
Anmerkung	gvOuId ((wie [ldapgvat] gvOrgUnit / gvOuId; siehe auch 6 Exkurs: IDs für Organisationen und Organisationseinheiten im österr. E-Government) der Organisationseinheit, die auch mit „3.3.3 Organisationskennzeichen der Organisationseinheit (OU-OKZ)“ beschrieben wird.
Syntax	gvOuID = Landeskennung ":" ID ID = "VKZ:" VKZ | Org-Id VKZ ::= 1#32UACHAR;(Verwaltungskennzeichen gem. [VKZ]) Org-Id ::= 1#32UACHAR;(Org-Id gem. [VKZ]) Landeskennung ::= 2#2ALPHA; (gem. ISO 3166 - Alpha2)
Länge	Max. 39 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.
Beispiele	AT:VKZ:GGA-1234 AT:L9:9876
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-GVOUID
PVP 1.9 XPATH-SOAP	authenticate/*Principal/gvOuId

3.3.5 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

Friendly Name	OU
HTTP Header Name	X-PVP-OU
Bedeutung	Kurzbezeichnung der mit ouGvOuId und ouOKZ referenzierten Organisationseinheit.
Syntax:	ou-value = {1-64} UTF_CHAR
Länge	Max. 64
Beispiele	I/11
XML-Schema-Type	xs:string
PVP 1.x HTTP Header außer 1.8	X-AUTHENTICATE-OU
PVP 1.8	-
PVP 1.9 XPATH-SOAP	authenticate/*Principal/Ou

3.3.6 Funktionsbezeichnung (FUNCTION)	
OID	1.2.40.0.10.2.1.1.33 (definiert durch ldap.gv.at)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.33
Friendly Name	FUNCTION
HTTP Header Name	X-PVP-FUNCTION
Bedeutung	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 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
Länge	Max. 32
Beispiele	FachbereichsleiterIn
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-AUTHENTICATE-GVFUNCTION
PVP 1.9 XPATH-SOAP	authenticate/userPrincipal/gvFunction

3.4 Berechtigungen / Autorisierung / Rollen

3.4.1 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
Friendly Name	ROLES
HTTP Header Name:	X-PVP-ROLES
Bedeutung	Beschreibt die PVP-Rollen, die den Benutzern von der zuständigen vom Participant beauftragen Rechteverwaltung zugeordnet wurden. Die möglichen Rollen einer Anwendung werden durch gvApplicationRight Objekte beschrieben.

<table>
<tr><td></td><td>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.</td></tr>
<tr><td>Syntax</td><td>Roles = Role *(„;“Role) [;]
Role = RoleName [„(„ [Parameters] “)”]
Parameters = Parameter [„„ Parameters]
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:
<table>
<tr><th>Zeichen</th><th>Kodierung</th><th>Beschreibung</th></tr>
<tr><td>,</td><td>\,</td><td>Comma</td></tr>
<tr><td>)</td><td>\)</td><td>Closing bracket</td></tr>
<tr><td>\</td><td>\\</td><td>Backslash</td></tr>
</table></td></tr>
<tr><td>Länge</td><td>Max. 32767
(Im Portalverbund der österreichischen Behörden gelten darüber hinaus die Maximallängenvorgaben aus der Konvention Rechtemodellierung [AG_IZ_Rechtemodell]</td></tr>
<tr><td>Beispiel</td><td>APP_ABFRAGE(GKZ=10000, GKZ=20000);APP_UPDATE(GKZ=50000)</td></tr>
<tr><td>Länge:</td><td>32767
(Im Portalverbund der österreichischen Behörden gelten darüber hinaus die Maximallängenvorgaben aus der Konvention Rechtemodellierung [AG_IZ_Rechtemodell])</td></tr>
<tr><td>XML-Schema-Type</td><td>xs:string</td></tr>
<tr><td>PVP 1.x HTTP Header</td><td>X-AUTHORIZE-ROLES</td></tr>
<tr><td>PVP 1.9 XPATH-SOAP</td><td>authorize/role</td></tr>
</table>

3.5 eID / Bürgerkartenspezifische Attribute

3.5.1 Deprecated - Authentifizierungslevel des Bürgers (EID-CITIZEN-QAA-LEVEL)

OID	1.2.40.0.10.2.1.1.261.94 definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.94
Friendly Name	EID-CITIZEN-QAA-LEVEL
HTTP Header Name	X-PVP-EID-CITIZEN-QAA-LEVEL
STORK Attribute	http://www.stork.gov.eu/1.0/citizenQAALevel
Bedeutung	Authentifizierungslevel des Bürgers nach [STORK D5.7.3].
Anmerkung	Im S-Profil wird das Authentifizierungslevel des Bürgers bei der Anmeldung als SAML AuthenticationContext wie in [SAML2IAProf] übermittelt. SAML-IdPs können die Sicherheitsklasse optional aber auch als Attribut übermitteln. Die Angabe des Authentifizierungslevels erfolgt im S-Profil nicht auf Basis von Integer-Werten, sondern auf Basis von URIs.
Mögliche Werte	Laut [STORK D5.7.3].
Syntax	qaa-value = DIGIT
Länge	1
Beispiel	4
XML-Schema-Type	*xs:integer*
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.2 Authentifizierungslevel des Bürgers (EID-CITIZEN-QAA-EIDAS-LEVEL)

OID	1.2.40.0.10.2.1.1.261.108 definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.108
Friendly Name	EID-CITIZEN-QAA- EIDAS-LEVEL
HTTP Header Name	X-PVP-EID-CITIZEN-QAA- EIDAS-LEVEL
eIDAS Attribute	Laut Response Element <saml2:AuthnContextClassRef> der eIDAS Assertion
Bedeutung	Authentifizierungslevel des Bürgers nach [STORK D5.7.3].
Anmerkung	Im S-Profil wird das Authentifizierungslevel des Bürgers bei der Anmeldung als SAML AuthenticationContext wie in [SAML2IAProf] übermittelt. SAML-IdPs können die Sicherheitsklasse optional aber auch als Attribut übermitteln.
Mögliche Werte	Laut [eIDAS-MsgFormat] D3.2.
Syntax	qaa-value = {64} UTF_CHAR
Länge	Max. 64
Beispiel	http://eidas.europa.eu/LoA/high
XML-Schema-Type	*xs:string*
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.3 EID Herausgebernation (EID-ISSUING-NATION)

OID	1.2.40.0.10.2.1.1.261.32; definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.32
Friendly Name	EID-ISSUING-NATION
HTTP Header Name	X-PVP-EID-ISSUING-NATION

Bedeutung	Staat, der das elektronische Identifikationsmedium herausgegeben hat, bzw. die Herausgabe regelt.
Mögliche Werte	Landescode gem. ISO-3166 ALPHA-2
Syntax	eid-issuing-nation-value = {2} ALPHA
Länge	2
Beispiel	AT
XML-Schema-Type	*xs:string*
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.4 Bereich und Typ des bereichsspezifischen Personenkennzeichens (EID-SECTOR-FOR-IDENTIFIER)

OID	1.2.40.0.10.2.1.1.261.34 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.34
Friendly Name	EID-SECTOR-FOR-IDENTIFIER
HTTP Header Name	X-PVP-EID-SECTOR-FOR-IDENTIFIER
Bedeutung	Das österreichische e-Government-Gesetz [E-GovG] sieht vor, dass verschiedene Bereiche der Verwaltung für natürliche Personen verschiedene Identifikatoren (=bPK; bereichsspezifisches Personenkennzeichen) verwenden müssen. Die Bereichsabgrenzungsverordnung regelt, in welche Bereiche die Verwaltung zu gliedern ist. Dieses Attribut gibt an, für welchen Verwaltungsbereich gem. Bereichsabgrenzungsverordnung [BerAbgrV] Personenkennzeichen berechnet wurden. Für den privatwirtschaftlichen Bereich wird für die Bereichskennung die Stammzahl des Auftraggebers herangezogen. Die Stammzahl des Auftraggebers entspricht der jeweiligen Registernummer, z.B. Firmenbuchnummer [E-GovG]. Siehe auch [bPK-Algo] bzw.[SZR].
Syntax	eid-id := bpk-eid-id | wbpk-eid-id | encrypted-eid-id bpk-eid-id := “urn:publicid:gv.at:cdid+”BEREICH wbpk-eid-id := WBPK-URN-PREFIX W-BEREICH encrypted-eid-id:= “urn:publicid:gv.at:ecdid+”VKZ “+” BEREICH BEREICH...Verwaltungsbereich gem. Bereichsabgrenzungsverordnung (siehe [BerAbgrV]) WBPK-URN-PREFIX := "urn:publicid:gv.at:wbpk+" SZ-TYPE "+"; URN-Prefix gem. Kap. "Ermittlung des Wirtschafts-bPK" [bPK-Algo] SZ-TYPE := "FN"|"VR|"ERJ"|"ZMR"|"ERN"; nicht normativ, wird in [bPK-Algo] spezifizier; Firmenbuch, Vereinsregister, Ergänzungsregister für sonstige Betroffene, Zentrales Melderegister, Ergänzungsregister für natürliche Personen W-BEREICH := 1#128 NAMECHAR; Stammzahl des Auftraggebers (siehe [E-GovG] bzw. [bPK-Algo]) VKZ := 1#32 NAMECHAR; Verwaltungskennzeichen
Länge	Max. 255
Beispiel	urn:publicid:gv.at:cdid+BW *(bPK)* urn:publicid:gv.at:wbpk+FN+468924i *(wbPK)* urn:publicid:gv.at:ecdid+BMI+BW (Fremd-bPK)
XML-Schema-Type	*xs:string*
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.5 Stammzahl der natürlichen Person (EID-SOURCE-PIN)	
OID	1.2.40.0.10.2.1.1.261.36; definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.36
Friendly Name	EID-SOURCE-PIN
HTTP Header Name	X-PVP-EID-SOURCE-PIN
Bedeutung	Stammzahl der natürlichen Person, die sich mithilfe eines staatlich anerkannten elektronischen Identifikationsmittels angemeldet hat. Der Begriff Stammzahl stammt aus dem österreichischen E-Government-Gesetz (E-GovG). Die Verwendung der Stammzahl natürlicher Personen ist i.B. durch §12 E-GovG streng beschränkt. Sie darf z.B. nicht gespeichert werden. Im Normalfall soll die Stammzahl nicht an Services – und wenn nur an behördliche - weitergeleitet werden. Anwendungen der öffentlichen Verwaltung müssen die bPK jenes Verwaltungsbereichs verwenden, dem die Anwendung im Zuge der datenschutzrechtlichen Abklärung zugerechnet wird. Anwendungen der Wirtschaft müssen einen speziell dem anwendungsverantwortlichen Unternehmen zugeordneten Identifier (wbPK) arbeiten. Der Typ der übertragenen Stammzahl wird dabei über das Attribut „EID-SOURCE-PIN-TYPE“ (siehe Abschnitt 3.5.6) angegeben. Derzeit existiert nur ein Typ.
Abhängigkeiten	Um dieses Attribut interpretieren zu können, muss auch das Attribute „EID-SOURCE-PIN-TYPE“ (siehe Abschnitt 3.5.6) angegeben werden
Syntax	eid-source-pin-value = {128} B64CHAR
Länge	Max. 128
Beispiel	dwGv1oNvB4BBkW/+G3eSEQ==
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.6 Art der Stammzahl der natürlichen Person (EID-SOURCE-PIN-TYPE)	
OID	1.2.40.0.10.2.1.1.261.104 definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid: 1.2.40.0.10.2.1.1.261.104
Friendly Name	EID-SOURCE-PIN-TYPE
HTTP Header Name	X-PVP-EID-SOURCE-PIN-TYPE
Bedeutung	Typ der Stammzahl bzw. Herkunft der Stammzahl der natürlichen Person. Derzeit existiert nur ein Typ.
Mögliche Werte	urn:publicid:gv.at:baseid
Syntax	eid-source-pin-value = {128} UTF_CHAR
Länge	Max. 128
Beispiel	urn:publicid:gv.at:baseid
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.7 Personenbindung (EID-IDENTITY-LINK)	
OID	1.2.40.0.10.2.1.1.261.38 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.38
Friendly Name	EID-IDENTITY-LINK
HTTP Header Name	X-PVP-EID-IDENTITY-LINK

Bedeutung	Gesamte Personenbindung der Person gemäß Konvention "XML Definition der Personenbindung" [PB] in Base64 Kodierung. Nachdem die Personenbindung die Stammzahl der natürlichen Person enthält, gelten dieselben Schutzregeln wie für die Stammzahl selbst (siehe Abschnitt 3.5.5).
Syntax	eid-identity-link-value = {32767} B64CHAR
Länge	Max. 32767
Beispiel	dwG…3eSEQ==
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.8 Für Authentifizierung signierte Nachricht (EID-AUTH-BLOCK)

OID	1.2.40.0.10.2.1.1.261.62 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.62
Friendly Name	EID-AUTH-BLOCK
HTTP Header Name	X-PVP-EID-AUTH-BLOCK
Bedeutung	Im österreichischen E-Government wird eine sichere Bürgerauthentifizierung auf Basis einer qualifizierten Signatur durchgeführt. Dieses Attribut enthält jenen Text, der von der BürgerIn während eines Authentifizierungsvorganges mittels qualifizierter eID signiert wurde.
Syntax	eid-auth-block-value = {32767} B64CHAR
Länge	Max. 32767
Beispiel	dwG…3eSEQ==
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.9 URL Bürgerkartenumgebung (EID-CCS-URL)

OID	1.2.40.0.10.2.1.1.261.64 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.64
Friendly Name	EID-CCS-URL
HTTP Header Name	X-PVP-EID-CCS-URL
Bedeutung	URL der für die Anmeldung verwendeten Bürgerkartenumgebung (BKU-URL). Kann verwendet werden, um z.B. beim Erstellen weiterer Signaturen im Rahmen der Anwendungsnutzung (z.B. Signieren von PDF Dokumenten) die Nutzung derselben Bürgerkartenumgebung vorzuschlagen bzw. zu erzwingen.
Syntax	eid-ccs-url-value = {1024} UTF_CHAR
Länge	Max. 1024
Beispiel	https://127.0.0.1:3496/https-security-layer-request
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.5.10 eID-Signatur-Zertifikat bei Authentifizierung (EID-SIGNER-CERTIFICATE)	
OID	1.2.40.0.10.2.1.1.261.66 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.66
Friendly Name	EID-SIGNER-CERTIFICATE
HTTP Header Name	X-PVP-EID-SIGNER-CERTIFICATE
Bedeutung	Base64 kodiertes Zertifikat, dass für die Anmeldung verwendet wurde. Mit Hilfe des Zertifikats kann ein SP beispielsweise überprüfen, ob es sich um ein qualifiziertes Zertifikat handelt oder ob eine bestimmte OID, welche z.B. die Eigenschaft eines berufsmäßigen Parteienvertreters abbildet, vorhanden ist.
Syntax	eid-signer-cert-value = {32767} B64CHAR
Länge	Max. 32767
Beispiel	MIIDXT…ZZKJEQxg==
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6 Vollmachten und Vertretungsrechte

3.6.1 Vollmachtentype (MANDATE-TYPE)	
OID	1.2.40.0.10.2.1.1.261.68 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.68
Friendly Name	MANDATE-TYPE
HTTP Header Name	X-PVP-MANDATE-TYPE
Bedeutung	Bezeichnung des verwendeten Vollmachten-Profils. Beschreibt den Umfang der Vollmacht bzw. Vertretungsbefugnis. Eine Liste von existierenden Vollmachten-Profilen kann unter [SRB] abgerufen werden.
Syntax	mandate-type-value = {256} NAMCHAR
Länge	Max. 256
Beispiele	PostvollmachtBilateral Einzelvertretungsbefugnis
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.2 Vollmachtentype-OID (MANDATE-TYPE-OID)	
OID	1.2.40.0.10.2.1.1.261.106 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.106
Friendly Name	MANDATE-TYPE-OID
HTTP Header Name	X-PVP-MANDATE-TYPE-OID
Bedeutung	Bezeichnung des verwendeten Vollmachten-Profils (siehe Abschnitt 3.6.1) als OID [OID]. Beschreibt den Umfang der Vollmacht bzw. Vertretungsbefugnis mittels eindeutigem Object Identifier. Werden sowohl MANDATE-TYPE als auch MANDATE-TYPE-OID verwendet, müssen beide Attribute miteinander konform gehen (siehe [SRB]). Eine Liste von existierenden Vollmachten-Profilen und der korrespondierenden OID kann unter [SRB] abgerufen werden.
Syntax	mandate-type-oid-value = {256} NAMCHAR
Länge	Max. 256
Beispiele	1.2.40.0.10.1.7.3.1.4 1.2.40.0.10.1.7.3.2.1.1
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.3 **Stammzahltyp der vertretenen natürlichen Person (MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE)**	
OID	1.2.40.0.10.2.1.1.261.102 definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.102
Friendly Name	MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE
Bedeutung	Typ der Stammzahl bzw. Herkunft der Stammzahl der vertretenen natürlichen Person. Derzeit existiert nur ein Typ. Siehe auch Abschnitt 3.5.6.
Mögliche Werte	urn:publicid:gv.at:baseid

Syntax	Mandatory-np-source-pin-type-value = {128} UTF_CHAR
Länge	128
Beispiel	urn:publicid:gv.at:baseid
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.4 Stammzahl der vertretenen natürlichen Person (MANDATOR-NATURAL-PERSON-SOURCE-PIN)

OID	1.2.40.0.10.2.1.1.261.70 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.70
Friendly Name	MANDATOR-NATURAL-PERSON-SOURCE-PIN
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-SOURCE-PIN
Bedeutung	Stammzahl der natürlichen Person, für die Vollmachts- bzw. Vertretungsbefugnisse ausgeübt werden. Das E-Government Gesetz sieht die Inklusion der Stammzahl der vertretenen natürlichen bzw. juristischen Person in einer elektronischen Vollmacht vor. Nachdem dieses Attribut die Stammzahl einer natürlichen Person enthält, gelten dieselben Schutzregeln wie in Abschnitt 3.5.5 beschrieben. Der Typ der übertragenen Stammzahl der vertretenen natürlichen Person wird dabei über das Attribut „MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE“ (siehe 3.6.3) angegeben. Derzeit existiert nur ein Typ.
Abhängigkeiten:	Dieses Attribut kann nur gemeinsam mit dem Attribut „MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE“ (siehe 3.6.3) interpretiert werden.
Syntax	mandator-natural-person-source-pin-value = {128} B64CHAR
Länge	Max. 128
Beispiele	NEK/9ZsnA7e2phK71F/OSdIjwbU=
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.5 Stammzahltyp der vertretenen juristischen Person (MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE)

OID	1.2.40.0.10.2.1.1.261.76 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.76
Friendly Name	MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE
HTTP Header Name	X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE
Bedeutung	Type von Stammzahl / Herkunft der Stammzahl Gibt an, um welche Art der Stammzahl einer vertretenen juristischen Person es sich handelt. Es wird unterschieden, ob die Stammzahl einer juristischen Person aus dem Firmenbuch (XFN), aus dem Zentralen Vereinsregister (XZVR) oder aus dem Ergänzungsregister für sonstige Betroffene (XERSB) stammt. [SZR]
Mögliche Werte	urn:publicid:gv.at:baseid+XFN *(Im Firmenbuch eingetragenes Unternehmen)* urn:publicid:gv.at:baseid+XZVR *(Verein gem. Vereinsregister)* urn:publicid:gv.at:baseid+XERSB *(Sonstige Einheit aus dem Ergänzungsregister sonstiger Betroffener)*

Syntax	m-lp-sp-value := BASE-ID "+" CORPORATE-TYPE BASE-ID := urn:publicid:gv.at:baseid CORPORATE-TYPE := "XFN" | "XZVR" | "XERSB"
Länge	128
Beispiel	urn:publicid:gv.at:baseid+XFN
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.6 Stammzahl der vertretenen juristischen Person (MANDATOR-LEGAL-PERSON-SOURCE-PIN)

OID	1.2.40.0.10.2.1.1.261.100 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.100
Friendly Name	MANDATOR-LEGAL-PERSON-SOURCE-PIN
HTTP Header Name	X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN
Bedeutung	Stammzahl der juristischen Person, für die Vollmachts- bzw. Vertretungsbefugnisse ausgeübt werden. Das E-Government Gesetz sieht die Inklusion der Stammzahl der vertretenen natürlichen bzw. juristischen Person in einer elektronischen Vollmacht vor. Der Typ der übertragenen Stammzahl der vertretenen juristischen Person wird dabei über das Attribut „MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE" (siehe 3.6.5) angegeben.
Abhängigkeiten	Kann nur gemeinsam mit dem Attribut „MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE" (siehe 3.6.5) interpretiert werden.
Syntax	mlp-source-pin-value = {128} NAMCHAR
Länge	Max. 128
Beispiele	123456d
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.7 Bereichsspezifisches Personenkennzeichen vertretene Person (MANDATOR-NATURAL-PERSON-BPK)

OID	1.2.40.0.10.2.1.1.261.98 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.98
Friendly Name	MANDATOR-NATURAL-PERSON-BPK
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-BPK
Bedeutung	Bereichsspezifisches Personenkennzeichen des Vollmachtgebers (siehe auch 3.2.6 Bereichsspezifisches Personenkennzeichen (BPK)). Nur wenn der Machtgeber eine natürliche Person ist.
Syntax / Länge / Beispiel	siehe 3.2.6 Bereichsspezifisches Personenkennzeichen (BPK)
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.8 Verschlüsselte Fremd-bPKs / Vertretene Person (MANDATOR-NATURAL-PERSON-ENC-BPK-LIST)

OID	1.2.40.0.10.2.1.1.261.72 Definiert durch PVP (dieses Dokument)

SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.72
Friendly Name	MANDATOR-NATURAL-PERSON-ENC-BPK-LIST
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-ENC-BPK-LIST
Bedeutung	Liste von Fremd-bPKs (=verschlüsselte bPKs) der vertretenen natürlichen Person in der unter Abschnitt 3.2.7 definierten Syntax.
Syntax	Siehe Abschnitt 3.2.7.
Länge	Siehe Abschnitt 3.2.7.
Beispiele	Siehe Abschnitt 3.2.7.
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.9 Vorname der vertretenen natürlichen Person (MANDATOR-NATURAL-PERSON-GIVEN-NAME)

OID	1.2.40.0.10.2.1.1.261.78 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.78
Friendly Name	MANDATOR-NATURAL-PERSON-GIVEN-NAME
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-GIVEN-NAME
Bedeutung	Vorname(n) der natürlichen Person, die die Vollmacht erteilt hat, bzw. die vertreten wird.
Syntax/ Länge / Beispiel	Siehe Abschnitt 3.2.2(Vorname (GIVEN-NAME))
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.10 Nachname der vertretenen natürlichen Person (MANDATOR-NATURAL-PERSON-FAMILY-NAME)

OID	1.2.40.0.10.2.1.1.261.80 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.80
Friendly Name	MANDATOR-NATURAL-PERSON-FAMILY-NAME
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-FAMILY-NAME
Bedeutung	Nachname der Person, die die Vollmacht erteilt hat, bzw. die vertreten wird.
Syntax / Länge / Beispiel	Siehe Abschnitt 3.2.1. (Bezeichnung / Nachname (PRINCIPAL-NAME))
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.11 Geburtsdatum der vertretenen natürlichen Person (MANDATOR-NATURAL-PERSON-BIRTHDATE)

OID	1.2.40.0.10.2.1.1.261.82 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.82
Friendly Name	MANDATOR-NATURAL-PERSON-BIRTHDATE
HTTP Header Name	X-PVP-MANDATOR-NATURAL-PERSON-BIRTHDATE
Bedeutung	Geburtsdatum der Person, die die Vollmacht erteilt hat, bzw. die vertreten wird.

Syntax / Länge / Beispiel	Siehe Abschnitt 3.2.3 (Geburtsdatum (BIRTHDATE))
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.12 Name der juristischen Person (MANDATOR-LEGAL-PERSON-FULL-NAME)

OID	1.2.40.0.10.2.1.1.261.84 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.84
Friendly Name	MANDATOR-LEGAL-PERSON-FULL-NAME
HTTP Header Name	X-PVP-MANDATOR-LEGAL-PERSON-FULL-NAME
Bedeutung	Name der juristischen Person bzw. Personenmehrheit gemäß zugrundeliegendem Register.
Syntax	Mandator-lp-full-name := {1-256} UTF_CHAR
Länge	Max. 256
Beispiel	G.E.B.O.L. Handels GmbH
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.13 Kennzeichnung berufsmäßiger ParteienvertreterInnen (MANDATE-PROF-REP-OID)

OID	1.2.40.0.10.2.1.1.261.86 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.86
Friendly Name	MANDATE-PROF-REP-OID
HTTP Header Name	X-PVP-MANDATE-PROF-REP-OID
Bedeutung	Liste von Object Identifiern (OID), zur Kennzeichnung von berufsmäßigen ParteienvertreterInnen bzw. OrganwalterInnen. Welche OID welche Berufsgruppe repräsentiert, wird durch die eGovernement Spezifikation „Object Identifier der öffentlichen Verwaltung“ [OID] festgelegt. Soll mehr als eine durch eine OID ausdrückbare Berufszugehörigkeit an eine Anwendung gemeldet werden, so werden die OIDs durch Strichpunkt (Semicolon, ";") voneinander getrennt. Die Verwendung von Leerzeichen (Whitespaces) ist dabei nicht vorgesehen.
Mögliche Werte:	1.2.40.0.10.3.1: Notarseigenschaft 1.2.40.0.10.3.2: Rechtsanwaltseigenschaft 1.2.40.0.10.3.3: Ziviltechnikereigenschaft 1.2.40.0.10.3.4: Organwaltereigenschaft 1.2.40.0.34.3.1.3: ELGA-Ombudsstelle (Produktivsystem) 1.2.40.0.34.3.1.2.99.9: ELGA-Ombudsstelle (Testsystem)
Syntax	Mandator-oid-value := {1-256} (OID [";" OID]) OID := {1-64} (DIGIT | “.”)
Länge	Max. 256
Beispiel	1.2.40.0.10.3.2;1.2.40.0.10.3.3 (Die angemeldete Person gehört sowohl der Berufsgruppe der RechtsanwältInnen als auch der der ZiviltechnikerInnen an.)
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.14 Beschreibung der berufsmäßiger ParteienvertreterInnen Eigenschaft (MANDATE-PROF-REP-DESCRIPTION)	
OID	1.2.40.0.10.2.1.1.261.88 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.88
Friendly Name	MANDATE-PROF-REP-DESCRIPTION
HTTP Header Name	X-PVP-MANDATE-PROF-REP-DESCRIPTION
Bedeutung	Textuelle Beschreibung der durch Abschnitt 3.6.13 bekanntgegebenen Eigenschaft als berufsmäßiger ParteienvertreterIn. Werden mehrere durch OIDs beschreibbare Berufszugehörigkeiten beschrieben, enthält das Attribut für jede OID eine Beschreibung, die durch Strichpunkt (Semicolon, ";") voneinander getrennt sind. Die Reihenfolge der Beschreibungstexte entspricht der Reihenfolge der OIDs.
Mögliche Werte:	Stand 2013 sind für folgende Berufsgruppen OID´s definiert: Notarseigenschaft Rechtsanwaltseigenschaft Ziviltechnikereigenschaft Organwaltereigenschaft
Syntax	mprDescValues=(mprDescValue *[";"mprDescValues]) mprDescValue = 1#128 ALPHA
Länge	Max. 1024
Beispiel	Rechtsanwaltseigenschaft;Ziviltechnikereigenschaft
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.15 Referenzwert für Revision (MANDATE-REFERENCE-VALUE)	
OID	1.2.40.0.10.2.1.1.261.90 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.90
Friendly Name	MANDATE-REFERENCE-VALUE
HTTP Header Name	X-PVP-MANDATE-REFERENCE-VALUE
Bedeutung	Defintion gem. [MIS]. „…enthält einen Wert (xs:token) zwischen 10 und 100 Zeichen (Buchstaben bzw. Ziffern), der die Signatur des Vertreters mit der Vollmachtenauswahl verkettet, d.h. der Vertreter muss diesen Wert auf Applikationsseite signieren." Die im Rahmen einer elektronischen Vollmachtserstellung generierte Transaktionsnummer. Die Transaktionsnummer erlaubt ein Audit beim Online Vollmachten-Service und sollte vom SP zur Revisionssicherheit mitprotokolliert werden.
Syntax	mandate-ref-value := 10#100 (DIGIT | ALPHA)
Länge	100
Beispiel	8540841758835392166
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.6.16 Vollmacht im XML Format (MANDATE-FULL-MANDATE-LIST)	
OID	1.2.40.0.10.2.1.1.261.92 Definiert durch PVP (dieses Dokument)
SAML-Attribute Name	urn:oid:1.2.40.0.10.2.1.1.261.92
Friendly Name	MANDATE-FULL-MANDATE
HTTP Header Name	X-PVP-MANDATE-FULL-MANDATE-LIST
Bedeutung	Liste von Base64 kodierten Vollmachten im XML Format gemäß Vollmachten-Spezifikation [Mandate]
Syntax	full-mandate-value := Base64 kodierte Vollmacht full-mandate-list := full-mandate-value [";" full-mandate-list]
Länge	Max. 32767
Beispiel	NEK…U=
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	Nicht verfügbar
PVP 1.x XPATH-SOAP	Nicht verfügbar

3.7 Verrechnungsrelevante Informationen

3.7.1 Rechnungsempfänger (INVOICE-RECPT-ID)	
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
Friendly Name	INVOICE-RECPT-ID
HTTP Header Name	X-PVP-INVOICE-RECPT-ID
Bedeutung	gvOuId (siehe auch 6 Exkurs: IDs für Organisationen und Organisationseinheiten im österr. E-Government) des Rechnungsempfängers.
Syntax	invoiceRecptId-value = {1-64} UACHAR
Länge	64
Beispiel	AT:B:102
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-ACCOUNTING-INVOICERECPTID
PVP 1.9 XPATH-SOAP	accounting/InvoiceRecptId

3.7.2 Kostenstellen (COST-CENTER-ID)	
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
Friendly Name	COST-CENTER-ID
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.
Syntax:	costCenterId-value = costCenterId-list | "<user defined>" costCenterId-list = ["<default>"] costCenterId *[";" costCenterId] [",<user defined>] costCenterId = 1#25 (NAMECHAR | SPACE | SLASH)
Länge	32767
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.
XML-Schema-Type	xs:string
PVP 1.x HTTP Header	X-ACCOUNTING-COSTCENTERID
PVP 1.9 XPATH-SOAP	accounting/CostCenterId

3.7.3 Gebührenstufe (CHARGE-CODE)

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
Friendly Name	CHARGE-CODE
HTTP Header 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.
Syntax:	chargeCode-value = ["<default>"] chargeCode *["," chargeCode] chargeCode = 1#2 DIGIT
Länge	32767
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.
XML-Schema-Type	xs:string

PVP 1.x HTTP Header	X-ACCOUNTING-CHARGECODE
PVP 1.9 XPATH-SOAP	accounting/ChargeCode

3.8 Reverse-Proxy Profil spezifische Parameter

3.8.1 Transaktionskennung (TXID)	
HTTP Header 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	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.
Beispiel	111231$3WQ@portal.lfrz.at
PVP 1.9 http Header Name	X-TXID (vor 1.9 war der Header nicht definiert)
PVP 1.9 XPATH-SOAP	pvpExtension/debug-ticket/txid

3.8.2 Protokoll der ursprünglich verwendeten URL (ORIG-SCHEME)	
HTTP Header Name	X-PVP-ORIG-SCHEME
Bedeutung	Protokollschema (http oder https) der URL, die vom Client für den Zugriff auf die angefragte Ressource verwendet hat.
Syntax	orig-scheme-value := {1-8} UACHAR
Länge	8
Beispiel	https
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

3.8.3 Hostname des ursprünglich verwendeten URL (ORIG-HOST)	
HTTP Header Name	X-PVP-ORIG-HOST
Bedeutung	Fully-Qualified Host Name (FQHN) inklusive Portangabe, sofern nicht der protokollspezifische Default-Port verwendet wurde. 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	orig-host := {1-256} UACHAR
Länge	Max. 256
Beispiel	portal.lfrz.at
PVP 1.9 HTTP Header	X-ORIG-HOSTINFO (vor 1.9 war der Header nicht definiert)
PVP 1.9 XPATH-SOAP	pvpExtension/orig-host/hostinfo

3.8.4 Pfad der ursprünglich verwendeten URL (ORIG-URI)	
HTTP Header Name	X-PVP-ORIG-URI
Bedeutung	Pfadteil des URL mit führendem "/" und ohne Query Parameter.
Syntax	orig-uri-value := {1-2048} UACHAR
Länge	Max. 2048
Beispiel	/at.lfrz.testapplication/start
PVP 1.9 http Header	X-ORIG-URI (vor 1.9 war der Header nicht definiert)
PVP 1.9 XPATH-SOAP	pvpExtension/orig-host/uri

3.8.5 Vom Stammportal verwendete Protokollbindungen	
HTTP Header Name	X-PVP-BINDING
Bedeutung	Art der Bindung des Tokens an den Request. Entweder HTTP, SOAP oder beide.
Syntax	bindings = binding *(„“binding) binding = 1#NameChar
Länge	Max. 32
Beispiel	http,soap
PVP 1.9 http Header	In PVP 1.x nicht definiert
PVP 1.9 XPATH-SOAP	nicht definiert, Header wird ausschließlich als HTTP-Header gesetzt

3.9 Erweiterte Angaben zum Benutzer nach eIDAS SAML Attribute Profile

Im Rahmen der Umsetzung der eIDAS Regulierung wurden viele personenbezogene SAML-Attribute sehr genau definiert. Soweit in PVP nicht schon eigene Attribute vorgesehen sind, sollen für diese Attribute keine eigenen PVP-Attribute vorgesehen werden, sondern direkt die eIDAS Spezifikationen [STORK D5.7.3] angewandt werden.

Für folgende Informationen sieht das eIDAS Attribute Profil bereits Attribute vor:

- Natürliche Personen
  - Geburtsname (http://eidas.europa.eu/attributes/naturalperson/BirthName)
  - Geburtsort (http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth)
  - Aktuelle Wohnadresse (http://eidas.europa.eu/attributes/naturalperson/CurrentAddress)
  - Geschlecht (http://eidas.europa.eu/attributes/naturalperson/Gender)
- Juristische Personen
  - Adresse (http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress)
  - VAT Registrierungsnummer (http://eidas.europa.eu/attributes/legalperson/VATRegistrationNumber)
  - Steuerreferenznummer (http://eidas.europa.eu/attributes/legalperson/TaxReference)
  - Directive 2012/17/EU Identifier (http://eidas.europa.eu/attributes/legalperson/D-2012-17-EUIdentifier)
  - Legal Entity Identifier (http://eidas.europa.eu/attributes/legalperson/LEI)
  - Economic Operator Registration and Identification (http://eidas.europa.eu/attributes/legalperson/EORI)
  - System for Exchange of Excise Data Identifier (http://eidas.europa.eu/attributes/legalperson/SEED)
  - Standard Industrial Classification (http://eidas.europa.eu/attributes/legalperson/SIC)
  -

4 Government und Citizen Token / Anwendungsfälle von PVP

Welche Attribute bei einem konkreten Zugriff übertragen werden, hängt vom jeweiligen Anwendungsfall ab. Für das S-Profil werden die zu übertragenden Informationen über die Metadaten je Service festgelegt.
Allgemein dürfen nur Informationen weitergegeben werden, deren Übermittlung zulässig ist und vom Empfänger benötigt werden (Minimalitätsprinzip).

4.1 PVP Government Token / Portalverbund der österreichischen Verwaltung

Das Portalverbundprotokoll entstand im Bereich der öffentlichen Verwaltung um Beschäftigten Zugriff auf Anwendungen anderer Behörden einzuräumen (G2G Anwendungsfälle, Governement (G) To (2) Governement(G)). Die Identität der zugreifenden Person muss in diesem Fall nachvollziehbar gehalten werden. Darum sind folgende PVP-Anmeldeattribute im Bereich G2G als verpflichtend (mandatory) vorgesehen:

- X-PVP-VERSION
- X-PVP-SECCLASS
- X-PVP-PARTICIPANT-ID
- X-PVP-GID
- X-PVP-USERID
- X-PVP-PRINCIPAL-NAME
- X-PVP-OU-GV-OU-ID
- X-PVP-OU

4.2 PVP Citizen Token / Portalverbund für Bürgerinnen und Bürger

Das Citizen Token beschreibt jene PVP-Attribute, die beim Zugriff durch Bürgerinnen bzw. Bürger zwischen Identity-Provider und Service-Provider ausgetauscht werden. Prinzipiell gilt in datenschutzrelevanten Zusammenhängen das Minimalitätsprinzip. D.h., es sollen von einem Identity-Provider nur jene personenbezogenen Daten übermittelt werden, deren Übermittlung gesetzlich vorgesehen ist, bzw. zu deren Übermittlung von den Betroffenen die ausdrückliche Zustimmung eingeholt wurde.
Dieser Abschnitt beschreibt typische Attributmengen für eine BürgerInnen-Authentifizierung. Diese typischen Attributmengen inkludieren all jene Attribute, die üblicherweise von E-Government Applikationen bei einer sicheren und eindeutigen BürgerInnen-Authentifizierung benötigt werden. Aus welchen Attributen das Citizen Token besteht hängt vom Anwendungsfall ab. In Folge werden zwei typische Anwendungsszenarien (reine BürgerInnen-Authentifzierung und BürgerInnen-Authentifzierung in Vertretung) beschrieben.

4.2.1 Citizen Token ohne Vertretungs- und Vollmachtsunterstützung

Für authentifizierungspflichtige Services, die die Nutzung mithilfe elektronischer Vollmachten bzw. Vertretungsrechte nicht unterstützen, besteht der *Citzen Token* typischerweise zumindest aus den folgenden PVP-Attributen:

- PVP-VERSION
- PRINCIPAL-NAME
- GIVEN-NAME
- BPK
- EID-CITIZEN-QAA-EIDAS-LEVEL
- EID-ISSUING-NATION
- EID-SECTOR-FOR-IDENTIFIER

4.2.2 Citizen Token mit Vertretungs- und Vollmachtsunterstützung

Anwendungen, die neben der persönlichen Anmeldung- auch die Nutzung elektronischer Vollmachten und Vertretungsrechte unterstützen, benötigen neben den unter Abschnitt 4.2.1 gelisteten Attributen zumindest noch folgende PVP-Attribute:

Unabhängig von der Rechtsform der vertretbaren Entität benötigte Attribute:

- MANDATE-TYPE
- MANDATE-TYPE-OID
- MANDATE-REFERENCE-VALUE
- MANDATE-PROF-REP-OID
- MANDATE-PROF-REP-DESCRIPTION

Für die Unterstützung der Vertretung natürlicher Personen benötigte Attribute:

- MANDATOR-NATURAL-PERSON-BPK
- MANDATOR-NATURAL-PERSON-GIVEN-NAME
- MANDATOR-NATURAL-PERSON-FAMILY-NAME
- MANDATOR-NATURAL-PERSON-BIRTHDATE

Für die Unterstützung der Vertretung juristischer Personen benötigte Attribute:

- MANDATOR-LEGAL-PERSON-SOURCE-PIN
- MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE
- MANDATOR-LEGAL-PERSON-FULL-NAME

4.2.3 Optionale Attribute des Citizen Token

PVP-Attribute dürfen nur dann in den *Citizen Token* für eine Zielanwendung aufgenommen werden, wenn die entsprechenden (z.B. datenschutzrechtlichen) Voraussetzungen gegeben sind. Alle möglichen zusätzlichen Attribute sind in der Übersichtstabelle in Abschnitt 7 gelistet.
Abhängigkeiten zwischen einzelnen PVP-Attributen sind dabei zu beachten (z.B.: Wird EID-SOURCE-PIN im *Citizen Token* übertragen, so MUSS auch EID-SOURCE-PIN-TYPE im *Citizen Token* inkludiert sein - dasselbe gilt für MANDATOR-NATURAL-PERSON-SOURCE-PIN und MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE).

5 Application Chaining

5.1 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:

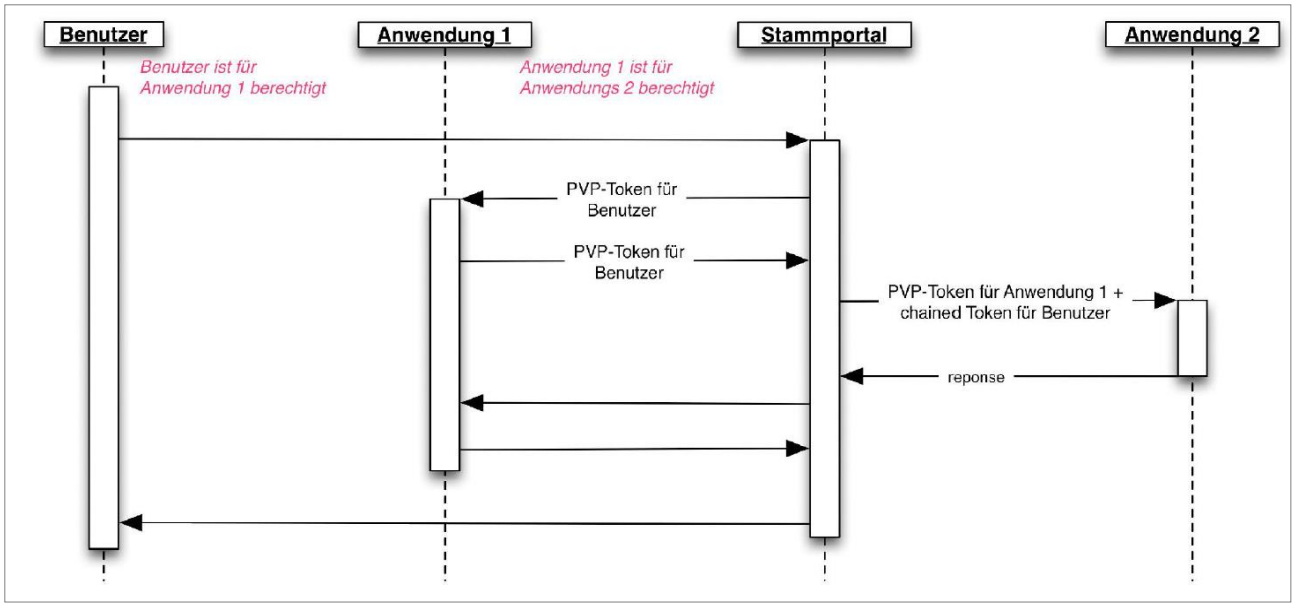

Abbildung 1 - Beispiel zu Chained-Token

Benutzer greift über Stammportal auf Anwendung-1 zu. Das Stammportal meldet Anwendung-1 die PVP-Informationen des Benutzers. Bei der Anmeldung von Anwendung-1 am Stammportal für den Zugriff auf Anwendung-2 wird der PVP-Token dem Benutzer 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 zum Endbenutzer beschreiben werden als *Chained Token* zusätzlich mitgeschickt.
Der *Chained Token* darf nicht zur Berechtigungsprüfung verwendet werden. Dafür muss der Token des direkten Zugriffspartners verwendet werden.

5.2 Chained Token in SAML Profilen

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

5.3 Attribute des Chained-Tokens

Der *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 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-VERSION wird nicht im *Chained Token* mitgeführt, da die *Chained Token* die gleiche Version wie der äußere Token haben müssen.

5.3.1 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 Prozess auslösenden Zugriff 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 in Abbildung 1 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 „02“ gekennzeichnet.

Attributnamen für den Chained Token im Reverse Proxy Profil
Die Attribute des *Chained Token* 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

6 Exkurs: IDs für Organisationen und Organisationseinheiten im österr. E-Government (nicht normativ)

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

6.1 Kennzeichen nach der Spezifikation VKZ

Für Organisationen und Organisationseinheiten der österreichischen Verwaltung wurden in der Spezifikation VKZ 1.2 [VKZ] zwei Kennzeichen eingeführt.

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

Im **OKZ/VKZ** ist Semantik enthalten.
Beispiel: Das OKZ/VKZ des Justizministeriums lautet „*BMJ*“
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** besteht aus einem Präfix, die den Herausgeber der Nummer kennzeichnet, und einer semantikfreien fortlaufende Nummer.
Beispiel: Die Org-ID des Justizministeriums lautet „*B:1*“.
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.

6.2 gvOuId – Schlüssel für Organisationen nach ldap.gv.at

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:GGA-1234, 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“

6.3 Zusammenfassung

Für Organisationen des 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.

7 Übersicht Token-Attribute

Die folgende Tabelle gibt einen Überblick über alle in PVP 2.1 verwendbaren Attribute und deren Einsatzmöglichkeiten im Rahmen der einzelnen Token-Varianten. Mit "M" werden erforderliche Attribute gekennzeichnet (Mandatory), mit "T" typische Attribute im Rahmen einer Authentifizierung.

PVP-Attribut	PVP Gov. Token	PVP Citizen Token	
		Ohne Vollmachten	Mit Vollmachten
PVP-VERSION	M	T	T
SECCLASS	M		
PRINCIPAL-NAME	M	T	T
GIVEN-NAME		T	T
BIRTHDATE			
USERID	M		
GID	M[5]		
BPK		T	T
ENC-BPK-LIST			
MAIL			
TEL			
PARTICIPANT-ID	M		
PARTICIPANT-OKZ			
OU-OKZ			
OU-GV-OU-ID	M		
OU	M		
FUNCTION			
ROLES			
Deprecated - ~~EID-CITIZEN-QAA-LEVEL~~		T	T
EID-CITIZEN-QAA-EIDAS-LEVEL			
EID-ISSUING-NATION		T	T
EID-SECTOR-FOR-IDENTIFIER		T	T
EID-SOURCE-PIN			
EID-SOURCE-PIN-TYPE			
EID-IDENTITY-LINK			
EID-AUTH-BLOCK			
EID-CCS-URL			
EID-SIGNER-CERTIFICATE			
MANDATE-TYPE			T
MANDATE-TYPE-OID			T
MANDATOR-NATURAL-PERSON-SOURCE-PIN			
MANDATOR-LEGAL-PERSON-SOURCE-PIN			T
MANDATOR-NATURAL-PERSON-SOURCE-PIN-TYPE			
MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE			T
MANDATOR-NATURAL-PERSON-BPK			T

[5] Nur für natürliche Personen ldap: gvOrgPerson bzw. in PVP im Userprincipal

PVP-Attribut	PVP Gov. Token	PVP Citizen Token	
		Ohne Voll-machten	Mit Voll-machten
MANDATOR-NATURAL-PERSON-ENC-BPK-LIST			
MANDATOR-NATURAL-PERSON-GIVEN-NAME			T
MANDATOR-NATURAL-PERSON-FAMILY-NAME			T
MANDATOR-NATURAL-PERSON-BIRTHDATE			T
MANDATOR-LEGAL-PERSON-FULL-NAME			T
MANDATE-PROF-REP-OID			T
MANDATE-PROF-REP-DESCRIPTION			T
MANDATE-REFERENCE-VALUE			T
MANDATE-FULL-MANDATE			
INVOICE-RECPT-ID			
COST-CENTER-ID			
CHARGE-CODE			
TXID			
ORIG-SCHEME			
ORIG-HOST			
ORIG-URI			
BINDING			

Anhang A 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; Version 1.0
http://www.ref.gv.at -> Portalverbund

[BerAbgrV]
Verordnung des Bundeskanzlers, mit der staatliche Tätigkeitsbereiche für Zwecke der Identifikation in E-Government-Kommunikationen abgegrenzt werden (E-Government-Bereichsabgrenzungsverordnung - E-Gov-BerAbgrV)
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003476

[bPK-Algo]
A. Hollosi, R. Hörbe: Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK) 1.1.1, 2007
http://reference.e-government.gv.at/uploads/media/Stammzahl-bPK-Algorithmen-1_1_1-20070131.pdf

[E-GovG]
Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG)
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230

[eIDAS-2015/1502]
COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

[eIDAS-AttrProfil]
eIDAS SAML Attribute Profile, Version 1.0, eIDAS Technical Sub-group, 22 June 2015 https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf

[eIDAS-MsgFormat]
eIDAS SAML Message Format Version 1.0 https://joinup.ec.europa.eu/sites/default/files/eidas_message_format_v1.0.pdf

[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

[Mandate]
Rössler, Hollosi, Liehmann, Schamberger: Elektronische Vollmachten Spezifikation 1.0.0, 2006

[MIS]
A.Tauber: Online-Vollmachten – Spezifikation 1.1.0, 2011
http://reference.e-government.gv.at/uploads/media/mis-1-1-0_20110929_01.pdf

[MOA-ID]
MOA-ID, Module für Online Applikationen-Identifikation, https://joinup.ec.europa.eu/software/moa-idspss/description

[OID]
Rössler, Pfläging, Pacnik: Object Identifier der öffentlichen Verwaltung – Teil 1 und 2,. 2009
http://reference.e-government.gv.at/AG-II-BK-OID-T1_OID-T2-1-0-0.2230.0.html

[PB]
A.Hollosi, G. Karlinger: XML Definition der Personenbindung 1.2.2 (2007)
http://reference.e-government.gv.at/uploads/media/xml-pb_1-2-2_20050214.pdf
[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

[RFC822]
D. Crocker & al.: " Standard for ARPA Internet Text Messages"
http://www.ietf.org/rfc/rfc0822.txt

[RFC1274]
Network Working Group, P.Barker, S. Kille: " The COSINE and Internet X.500 Schema", Nov. 1991,
http://www.ietf.org/rfc/rfc1274.txt

[RFC2616]
R. Fielding & al.: Hypertext Transfer Protocol -- HTTP/1.1
http://www.ietf.org/rfc/rfc2616.txt

[RFC2798]
Network Working Group, M. Smith: "Definition of the inetOrgPerson LDAP Object Class", April 2000;
http://www.ietf.org/rfc/rfc2798.txt

[RFC4517]
Network Working Group, S. Legg, Ed., "LDAP – Syntax and Matching Rules", Juni 2006

[RFC4519]
A. Sciberras: Lightweight Directory Access Protocol (LDAP): Schema for User Applications
http://www.ietf.org/rfc/rfc4519.txt

[RFC4524]
K. Zeilenga: COSINE LDAP/X.500 Schema
http://www.ietf.org/rfc/rfc4524.txt

[SAML20]
Oasis, SAML Version 2.0, März 2005, Errata Version verfügbar
http://saml.xml.org/saml-specifications

[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

[SRB]
Stammzahlenregisterbehörde: Unterstützte Profilgruppen und unterstützte Einzelprofile. https://voll-machten.stammzahlenregister.gv.at/mis/

[STORK D5.7.3]
STORK Konsortium: D5.7.3 Functional Design for PEPS, MW models and interoperability, 2011.
https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1874

[SZR]
O. Ehrenmüller: SZR 2.0 Anwendungsdokumentation
http://szr.bmi.gv.at/ref/portref/files/anleitungen/szr-2.0-anwenderdokumentation.pdf

[VKZ]
Grandits: Verwaltungskennzeichen:
http://reference.e-government.gv.at / Dokument VKZ 1.2.0

[XML DSIG]
W3C: "XML Signature Syntax and Processing (Second Edition)", Juni 2008
http://www.w3.org/TR/xmldsig-core/

[XML-ENC]
W3C: " XML Encryption Syntax and Processing", Dezember 2002
http://www.w3.org/TR/xmlenc-core/