

Wirtschaftsportalverbund Attribute

Version 1.0, 2016-02-29 (Entwurf)

Editor: Rainer Hörbe

Beiträge von: Franz Grandits

Um die Einbindung von Anwendungen und Identitätsprovidern möglichst einfach zu gestalten, werden Attributprofile definiert, um die Behandlung einzelner Attribute einzusparen. Die Basis für die Attributprofile ist ein Katalog, der übergreifend für die Profile verwendet werden kann.

Anmerkung: Attribute in SAML sind synonym mit Claims in der Microsoft-Welt.

1 Katalog der Attribute

Attribut/OID	Beschreibung (<i>Beispiel</i>)	Länge
commonName 2.5.4.3	Vorname Familienname	64
displayName 2.16.840.1.113730.3.1.241	Format „Familienname, Vorname“	64
surname 2.5.4.4	Familienname	64
givenName 2.5.4.42	Vorname	64
uid 0.9.2342.19200300.100.1.1	Innerhalb der Domäne eindeutige Benutzerkennung plus Domain-Suffix im RFC 822-Format. Der Wert ist meistens eine gültige Emailadresse. (<i>mmustermann@abcxyz.at</i>)	256
gid 1.2.40.0.10.2.1.1.1	Global eindeutiger Identifier bestehend aus: ‚AT:‘, einem Präfix, der den Namensraum bezeichnet, ‚:‘ als Trennzeichen, sowie einem zumindest innerhalb des Namensraumes unverwechselbar einer Person zuordenbarem Identifier. (<i>AT:WKIS:12356789</i>)	128
wbpkHash 1.2.40.0.10.2.1.1.149	Global eindeutiger Identifier bestehend aus: ‚AT:WBPK{SHA1}:‘, der Stammzahl des Auftraggebers von dem das bPK erstellt wurde, einem ‚:‘ als Trenner sowie der SHA1-Ableitung der wbPK der Bürgerkarte. (<i>AT:WBPK{SHA1}:468924i :j/NxdRQhp+tNyE9WhHdBSYuy3hA=</i>)	64
gender 1.3.6.1.4.1.1466.115.121.1.27	Geschlecht der Person (ISO 5218). Format: 0 Not known 1 Male 2 Female 9 Not specified	integer
title 2.5.4.12	Akademischer Titel (vorangestellt) (<i>Mag. d. s. K.</i>)	64
intTitle (oid t.b.d.)	Internationaler (nachgestellter) akademischer Titel (<i>LLM</i>)	40

telephoneNumber 2.5.4.20	Tel-Nummer(n) nach RFC2252 Abs 6.30 Format: +LL VVVV AAAAAA NNNN L: Land; V: Vorwahl; A: Anschluss; N: Nebenstelle	32
mail 0.9.2342.19200300.100.1.3	Email-Adresse im RFC 822-Format. (<i>mmustermann@abcxyz.at</i>)	256
Street 2.5.4.9	Straße der Postanschrift (<i>Bahnhofstr. 1</i>)	128
postOfficeBox 2.5.4.18	Postfach der Postanschrift (<i>Postfach 103</i>)	40
postalAddress 2.5.4.16	Postanschrift ohne Name Format: (6 Zeilen á 40 Zeichen; Zeilenende mit \$) (<i>Hintere Salzamtstraße 1\$1030 Wien</i>)	245
postalCode 2.5.4.17	Postleitzahl der Postanschrift ohne Ländercode (<i>1082</i>)	13
locality 2.5.4.7	Ort (<i>Wien</i>)	64
country 2.5.4.6	Land 2-stelliger ISO 3166 Code (<i>AT</i>)	2
orgSourcePin 1.2.40.0.10.2.1.1.261.100	Stammzahl (Firmenbuchnummer, Vereinsregisternummer, Zahl Ergänzungsregister). Format: URN-Präfix der wbPK plus Registerzahl ohne Blanks. URN-Präfix := "urn:publicid:gv.at:wbpk+XXX+" Wobei 'XXX': o XFN für das Firmenbuch o XVR für das Vereinsregister o XERSB für das Ergänzungsregister sonst. Betroffene (<i>urn:publicid:gv.at:wbpk+FN+318886a</i>)	64
gln 1.3.88	Global Location Number (Die GLN könnte von der im Unternehmensregister vergebenen abweichen, wenn ein Unternehmen seinen Nummernblock direkt von der GS1 bezieht.)	13
organizationName 2.5.4.10	Organization Name (<i>Identinetics IT-Services GmbH</i>)	128

rights 1.2.40.0.10.2.1.1.261.30	<p>Liste der dem Benutzer für eine Anwendung gewährten Rechte einschließlich der dazugehörigen Parameter.</p> <p>EBNF-Syntax:</p> <pre> Roles = Role * (";"Role) [;] Role = RoleName ["(" [Parameters] ")"] Parameters = Parameter ["," Parameters] Parameter = ParameterName "=" ParameterValue RoleName = 1#NameChar ParameterName = 1#NameChar ParameterValue = 1#UTF_CHAR </pre> <p>Regel für Parameterwerte: Die Zeichen ,) \ müssen in Parameterwerten kodiert werden, indem ein Backslash (\) vorangestellt wird.</p> <p>Drei Beispiele:</p> <pre> APP_ADMIN APP_READ(Region=EMEA);APP_UPDATE(Region=AT) APP_READ(Region=AT,Region=CH) </pre>	32767
registrationClassOrg OID t.b.d	<p>Registrierungsqualität juristische Person:</p> <ol style="list-style-type: none"> 1 Selbstregistrierung 2 mit Ausweisvorlage 3 geprüft gegen ein Register 	int
registrationClassUser OID t.b.d	<p>Registrierungsqualität natürliche Person:</p> <ol style="list-style-type: none"> 1 Selbstregistrierung / Registrierung durch ein angeschlossenes Unternehmen 2 mit Vorlage entsprechender Unterlagen (Firmenbuchauszug, ZVR-Auszug) 3 geprüft gegen ein Register 	int
authenticationClass OID t.b.d	<p>Authentifizierungsqualität</p> <p>1FA Ein Faktor (Passwort)</p> <p>QC Qualifiziertes Zertifikat (Bürgerkarte)</p>	20

2 Attributprofil „WKIS“

Für die Anwendungen die mit dem WKIS-IDP der WKO aufgesetzt werden, wird dieses Profil definiert. Das Attributprofile kann über die EntityCategory „<http://wirtschaftsportalverbund.at/namespaces/>

Attribut/OID	WKIS Claim
commonName 2.5.4.3	
displayName 2.16.840.1.113730.3.1.241	Anzeigenname
surname 2.5.4.4	
givenName 2.5.4.42	
uid 0.9.2342.19200300.100.1.1	UserPrincipalName
gid 1.2.40.0.10.2.1.1.1	PersonID
wbpkHash 1.2.40.0.10.2.1.1.149	
gender 1.3.6.1.4.1.1466.115.121.1.27	Gender
personalTitle 2.5.4.12	PersonTitle
telephoneNumber 2.5.4.20	
mail 0.9.2342.19200300.100.1.3	Email
postalAddress 2.5.4.16	
country 2.5.4.6	„AT“
orgSourcePin 1.2.40.0.10.2.1.1.261.100	Ableitung von Firmenbuchnummer (wenn vorhanden)
gln 1.3.88	GLN
rights 1.2.40.0.10.2.1.1.261.30	Ableitung von Role
registrationClassOrg	

WPV Attribute

registrationClassUser

authenticationClass