Wirtschaftsportalverbund

Attribute

Version 1.4, 2019-05-21

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.

1 Katalog der Attribute

1.1 Benutzerbezogene Attribute

Attribut/OID	**Beschreibung *(Beispiel)***	**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 und soll im RFC 822-Format geschrieben werden. Der Wert ist meistens eine gültige Emailadresse. *(mmustermann@abcxyz.at)*	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 und dauerhaft einer Person zuordenbarem Identifier. *(AT:WKIS:12356789)*	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. *(AT:WBPK{SHA1}:468924i :j/NxdRQhp+tNyE9WhHdBSYuy3hA=)*	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) *(Mag. d. s. K.)*	64

intTitle 1.2.40.0.10.2.1.1.229	Internationaler (nachgestellter) akademischer Titel *(LLM)*	64 (single valued)
telephoneNumber 2.5.4.20	Tel-Nummer(n) nach RFC2252 Abs 6.30 Format: +LL VVVV AAAAAAA NNNN L: Land; V: Vorwahl; A: Anschluss; N: Nebenstelle	32
mail 0.9.2342.19200300.100.1.3	Email-Adresse im RFC 822-Format. *(mmustermann@abcxyz.at)*	256
Street 2.5.4.9	Straße der Postanschrift *(Bahnhofstr. 1)*	128
postOfficeBox 2.5.4.18	Postfach der Postanschrift *(Postfach 103)*	40
postalAddress 2.5.4.16	Postanschrift ohne Name Format: (6 Zeilen á 40 Zeichen; Zeilenende mit $) *(Hintere Salzamtstraße 1$1030 Wien)*	245
postalCode 2.5.4.17	Postleitzahl der Postanschrift ohne Ländercode *(1082)*	13
localityName 2.5.4.7	Ort *(Wien)*	64
country 2.5.4.6	Land 2-stelliger ISO 3166 Code *(AT)*	2

rights
1.2.40.0.10.2.1.1.261.30
	Liste der dem Benutzer für eine Anwendung gewährten Rechte einschließlich der dazugehörigen Parameter.
	EBNF-Syntax:
	`Roles = Role *(";"Role) [;]`
	`Role = RoleName ["(" [Parameters] ")"]`
	`Parameters = Parameter ["," Parameters]`
	`Parameter = ParameterName "=" ParameterValue`
	`RoleName = 1#NameChar`
	`ParameterName = 1#NameChar`
	`ParameterValue = 1#UTF_CHAR`
	Regel für Parameterwerte:Die Zeichen ,);\ müssen in Parameterwerten kodiert werden, indem ein Backslash (\) vorangestellt wird.
	Drei Beispiele:
	APP_ADMIN
	APP_READ(Region=EMEA);APP_UPDATE(Region=AT)
	APP_READ(Region=AT,Region=CH)
		32767

registrationClassUser http://wirtschaftsportalverbund.at/ns/identity/claims/2016/04/registrationClassUser	Registrierungsqualität natürliche Person: 1 Selbstregistrierung / Registrierung durch ein angeschlossenes Unternehmen 2 mit Vorlage entsprechender Unterlagen (Firmenbuchauszug, ZVR-Auszug) 3 geprüft gegen ein Register	int
authenticationClass http://wirtschaftsportalverbund.at/ns/identity/claims/2016/04/authenticationClass	Authentifizierungsqualität 1FA Ein Faktor (Passwort) QC Qualifiziertes Zertifikat (Bürgerkarte)	20

1.2 Unternehmensbezogene Attribute

In diesem Zusammenhang kann das Unternehmen auch eine natürliche Person sein, für die eine andere Person tätig wird.

Attribut+OID/URI	**Beschreibung *(Beispiel)***	**Länge**
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 *(Identinetics IT-Services GmbH)*	128
registrationClassOrg http://wirtschaftsportalverbund.at/ns/identity/claims/ 2016/04/ registrationClassOrg	Registrierungsqualität juristische Person: 1 Selbstregistrierung 2 mit Ausweisvorlage 3 geprüft gegen ein Register	int
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 *(urn:publicid:gv.at:wbpk+FN+318886 a)*	64

1.3 Qualitäten der Identifier

In der nachfolgenden Tabelle werden die Eigenschaften der Identifier zusammengefasst:

1. Eindeutig
2. Dauerhaft (gilt für Lebensdauer der Entität)
3. Nicht wiederverwendbar (kann keiner anderen Entität zugewiesen werden)
4. Bereichs-/servicespezifisch (gilt nur für ein Service oder ein Gruppe von Services, im Gegensatz zu einem globalen Identifier)
5. UI-geeignet (kann von Benutzern leicht gelesen oder geschrieben werden)

Identifier	1	2	3	4	5
uid	X				
gid	X	X			
wbpk	X	X	X	X	
wpbkHash	X	X	X		
gln	X	X			X
orgSourcePin	X	X	X		
email	X				X

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 in den Metadaten referenziert werden: http://wirtschaftsportalverbund.at/namespaces/ecStandardAttributes/20160322

Ein Benutzer meldet sich am WKIS im Kontext eines Mitglieds (das ist ein Unternehmen, oder eine Niederlassung in einem Bundesland) an. Daher beziehen sich die Kontaktdaten auf diese Auswahl.

Attribut/OID	**WKIS Claim**[1]	**Abh.**[2]
commonName 2.5.4.3	Anzeigename (Titel, Vorname, Nachname, nachgestellter Titel)	
displayName 2.16.840.1.113730.3.1.241	Abgeleitet	
surname 2.5.4.4	surname	
givenName 2.5.4.42	givenname	
uid 0.9.2342.19200300.100.1.1	UPN (UserPrincipalName), enthält Email	
gid 1.2.40.0.10.2.1.1.1	PersonID (UUID)	
wbpkHash 1.2.40.0.10.2.1.1.149	Abgeleitet aus bPK	
gender 1.3.6.1.4.1.1466.115.121.1.27	Gender	
personalTitle 2.5.4.12	title	
mail 0.9.2342.19200300.100.1.3	Email	
postalAddress 2.5.4.16	Zustelladresse des gewählten Mitglieds	X
country 2.5.4.6	(aus Adresse)	X
orgSourcePin 1.2.40.0.10.2.1.1.261.100	Ableitung von Firmenbuchnummer (wenn vorhanden)	X
gln 1.3.88	GLN	X
organizationName 2.5.4.10	Organization Name *(Identinetics IT-Services GmbH)*	128

[1] Anmerkung: Attribute in SAML sind synonym mit Claims in der Microsoft-Welt

[2] Abhängig von der Rollenauswahl; d.h., dass ohne Rollenauswahl das Attribut nicht übermittelt wird

<table>
<tr><td>rights
1.2.40.0.10.2.1.1.261.30</td><td>Ableitung von Role</td><td>X</td></tr>
<tr><td>registrationClassOrg
http://wirtschaftsportalverbund.at/ns/identity/claims/2016/04/ registrationClassOrg</td><td>Immer auf 3 (gegen GISA geprüft)</td><td>X</td></tr>
<tr><td>registrationClassUser
http://wirtschaftsportalverbund.at/ns/identity/claims/2016/04/registrationClassUser</td><td>
<table>
<tr><th colspan="2">WKIS</th><th colspan="2">WPV</th></tr>
<tr><td>0</td><td>Selbstbeh.</td><td>1</td><td>Selbstbehaupt.</td></tr>
<tr><td>1</td><td>Bürgerkarte</td><td>4</td><td>Gegen Register geprüft</td></tr>
<tr><td>2</td><td>Postzustell.</td><td></td><td></td></tr>
<tr><td>3</td><td>Dok-qual.</td><td>3</td><td>Ausweisvorlage</td></tr>
<tr><td>4</td><td>Vorsystem (Gründers.)</td><td>3</td><td>Ausweisvorlage</td></tr>
</table>
</td><td></td></tr>
<tr><td>authenticationClass
http://wirtschaftsportalverbund.at/ns/identity/claims/2016/04/authenticationClass</td><td></td><td></td></tr>
<tr><td>PossibleRoles
http://schemas.wko.at/ws/2014/06/identity/claims/possiblerole</td><td>PossibleRoles lt . Einbindungsdokumentation - Anhang Claims WKIS 2</td><td></td></tr>
</table>

2.1 Redirect Claim

http://schemas.wko.at/ws/2014/02/identity/claims/redirect

Auf Grund technischer Einschränkungen muss nach einer Authentifizierung in manchen Fällen nach der Übermittlung des SAML Response noch eine zusätzliche Benutzerinteraktion mit dem WKIS IDP gemacht werden. Hierbei handelt es sich um eine http(s)-Adresse. Der Redirect-Claim wird in folgenden Situationen ausgestellt und beinhaltet je nach Situation unterschiedliche Werte:

- Der Benutzer muss seine Stammdaten ergänzen
- Der Login erfolgte über eine nicht zugeordnete Bürgerkarte
- Zur Rollenauswahl – diese geschieht entweder implizit (wenn der Benutzer nur eine Rolle besitzt) oder explizit (der Benutzer wählt manuell eine von mehreren Rollen aus) Wird ein Redirect-Claim ausgestellt, so muss die Anwendung darauf reagieren.

Beispielwert: https://tae.dev.oe.wknet/MyWkisFrontend/RoleSelection/RoleSelection.aspx

Details siehe Kapitel 2.2, Technische Behandlung des Redirect-Claims.

3 EntityCategories

Für das Attributprofil „WKIS“ wird folgende EntityCategory festgelegt:

http://wirtschaftsportalverbund.at/ns/ec/attributebundle-wkis

Mittels der EntityCategory wird ein Bündel von Attributen festgelegt, ohne diese einzeln in den Metadaten listen zu müssen, was nämlich ohne Unterstützung von Werkzeugen in XML im Allgemeinen schwer lesbar ist. Die Freigabe von Attributen im IDP erfolgt daher auf Basis der in den SP-Metadaten angegebenen EntityCategory.

4 Änderungshistorie

Version	Autor	Datum	Stichworte
1.0	R. Hörbe	2016-04-08	Freigabe mit Abschluss des Projekts „WPV 2015“
1.1	R. Hörbe	2016-04-12	Ergänzung EntityCategory
1.2	R.Hörbe	2016-05-23	Ergänzung URI für WKIS-Attribute
1.3	R.Hörbe	2016-12-13	Ergänzung intTitle OID
1.4	R. Hörbe	2019-05-23	Ergänzung Org-Attribute in WKIS-Profil

5 Referenzen

[draft-young-entity-category-02] IEFT; The Entity Category SAML Attribute Types, July 2014. https://tools.ietf.org/html/draft-young-entity-category-02