Benutzerattribute im F-IAM

IAM - Identity and Access Management

Exported on 10/15/2024

Table of Contents

1 Prozess zum Einführen neuer Benutzerattribute

1. Die Anwendung meldet den Bedarf an den Basisdienst IAM (di-pg-iam@bka.bund.de[1])
2. Der Basisdienst IAM prüft die Anforderung
    - Wird der Bedarf nicht bereits durch existierende Attribute abgedeckt?
    - Ist die Anforderung berechtigt? (Gehört die Information zum Benutzer und nicht beispielsweise zur Dienststelle des Benutzers?)
3. Bei positivem Prüfergebnis:
    - Legt der Basisdienst IAM fest, wie das neue Benutzerattribut übertragen werden kann und dokumentiert dies auf dieser Seite
        - von den TN an das F-IAM per TN-LDAP und/oder TN-SCIMv2
        - von dem F-IAM an die AW, z.B. per AW-SCIMv2 oder JTW
    - Wird das F-IAM für diese Übertragung ertüchtigt
    - Wenn das neue Attribut für die Anwendung ein Pflichtfeld ist, wird ein Defaultwert vereinbart, den das F-IAM für Benutzer mit einem leeren Wert einträgt. Die Verantwortung zur Klärung, wie mit diesem Wert umzugehen ist, liegt bei den Anwendungsverantwortlichen.
4. Teilnehmer, die auf die Anwendung mit dem neuen Bedarf zugreifen wollen, verantworten selbst, dass das Benutzerattribut geeignet befüllt wird.

1 mailto:di-pg-iam@bka.bund.de

2 Aktuelle Liste

Die farblich hervorgehobenen Einträge sind noch Gegenstand aktueller Abstimmungen und damit nicht verbindlich.

Bezeichnung (*: Pflichtfeld)	**Status**	**TN-LDAP Attribut**	***-SCIMv2-Attribut (Planungsstand)**	**OIM-Attributname**	**OAM-Attribut**	**JWT-Claim (im F-IAM-Token)**	**Datentyp**	**Beispiel**	**Bemerkung**
Pfad im Verzeichnisdienst*		-	-	dn	name	-	String-1024	uid=an4711123,ou=AN,ou=App,dc=bka,dc=bund,dc=de	Wird automatisch durch den Verzeichnisdienst gebildet
Nutzerkennung*	Berechnet	Ermittelt aus userPrincipalName ohne Domain mit vorgestellter TN-Kennung	userName	User Login	uid	sub	String-256	an4711123	
Allgemeiner Name	Berechnet	-	-	Common Name	cn	-	String-256	an4711123	Wird bisher nur F-IAM-intern verwendet

TN-interner Nutzername*	Vorhanden	userPrincipalName	urn:...:p20:user.idpUserName	UserPrincipalName	krbPrincipalName	-	String-80	4711123@police-an.de[2]	Dieser Wert muss vom TN im sub-Claim des TN-Access-Tokens übertragen werden
P-Kennung	Vorhanden	-	-	?	-	-	String	TODO	Wird vom F-IAM bei Bedarf als zufällige ID für die SZ4 generiert Wird als einziges Benutzerattribut in die SZ4 übertragen
TN-interne Nutzer-ID	WIP	-	urn:...:p20:user.idpUserId	TODO	TODO	-	TODO		z.B. TN-interne Anmeldekennung, sofern sie sich im TN-AD von dem userPrincipalName unterscheidet
Titel	Vorhanden	title	title	Title	title	-	String-30	(keine Testdaten vorhanden)	Neu aufgenommen

2 mailto:alfons.zitterback@police-an.de

Nachname*	Vorhanden	sn	name.familyName	LastName	sn	family_name	String-80	Zitterbacke	Bei der Zulieferung durch die TN über LDAP sind in diesem Feld weiterer Namensbestandteile wie "von", "II." enthalten. Bei SCIMv2 sind dafür dedizierte Felder der Struktur name zu verwenden.
Vorname*	Vorhanden	givenName	name.givenName	FirstName	givenName	given_name	String-80	Alfons	
Spitzname	Vorhanden	-	-	MiddleName	initials	-	String-80	(keine Testdaten vorhanden)	Wird nur zentral im OIM gepflegt, nur für EKUS

Namensvorsatz	WIP	-	name.honorificPrefix	TODO	TODO	-	TODO	Dr.	Diese Namensbestandteile können nur per SCIMv2 übertragen werden. Bei einer TN-LDAP-Anbindung müssen sie bei Bedarf mit in eines der anderen Namensfelder aufgenommen werden.
Namenszusatz	WIP	-	name.honorificSuffix	TODO	TODO	-	TODO	Jr., III.	
P20-Namenszusatz	WIP		urn:...:p20:user.nameSuffix					1 / 2	Das Feld kann dazu genutzt werden, Benutzer desselben TN mit identischem Namen zu unterscheiden. (Wurde konkret für IGVP eingeführt.)
EMail-Adresse*	Vorhanden	mail	emails[type eq "work"].value	Email	mail	email	String-245	alfons.zitterbacke@bka.bund.de[3]	Der Wert muss über alle Benutzer eindeutig sein.

3 mailto:alfons.zitterbacke@bka.bund.de

Telefonnummer	Vorhanden	telephoneNumber	phoneNumbers[type eq "work"].value	Telephone	telephoneNumber	phone_number	String-20	+49 (0)177 1234 567	
CNP-Telefonnummer	WIP	policeCnpTelephoneNumber	phoneNumbers[type eq "cnp"].value					7-207-2899	
Faxnummer	Vorhanden	facsimileTelephoneNumber	phoneNumbers[type eq "fax"].value	Fax	facsimileTelephoneNumber	fax_number			neu für Artus
Sprache	Vorhanden	-	-	CommunicationLanguage	preferredLanguage	-	String-50	en	

Organisationseinheit (DEPRECATED)	Vorhanden	ou	urn:...:Enterprise:user.organization	Organisational Unit	ou	organizational_unit	String-256	PP	Dienststelleninformation der gröbsten Ebene **DEPRECATED** wird schnellstmöglich durch P20-Dienststellenschlüssel ersetzt
Bereich (DEPRECATED)	Vorhanden	division	urn:...:Enterprise:user.division	Division	physicalDeliveryOfficeName	division	String-1024		Dienststelleninformation der mittleren Ebene **DEPRECATED** wird schnellstmöglich durch P20-Dienststellenschlüssel ersetzt
Abteilung (DEPRECATED)	Vorhanden	department	urn:...:Enterprise:user.department	Department	departmentNumber	department_number	String-1024		Dienststelleninformation der feinsten Ebene **DEPRECATED** wird schnellstmöglich durch P20-Dienststellenschlüssel ersetzt

P20-Dienststellenschlüssel	WIP	policeOfficeIdentifier	urn:...:p20:user.p20DepartmentNumber	OfficeIdentifier	policeOfficeIdentifier	p20_department_number	TODO		Neues Feld. Wird perspektivisch auf den P20-Dienststellenkatalog verweisen, kann aber unabhängig davon schon genutzt werden. **Schema-Erweiterung noch ausstehend**
Anzeigename	Berechnet	-	-	TODO	displayName	display_name	TODO		Automatisch gebildet aus Vor- und Nachname
Lokation	Vorhanden	-	-	Location	l	-	String-1000	(keine Testdaten vorhanden)	Wird aktuell weder ausgelesen noch ausgewertet
Anonyme Nutzerkennung	Berechnet	-	-	AnonymizedLogin	policeAnonymousName	-	String-64	p4711123	Nutzername für SZ4 wird OIM-intern generiert

Amtsbezeichnung	WIP	policeTitleKey	urn:...:p20:user.policeTitleKey						Verweis auf Katalog
P20-UID	WIP	policeUserIdentifier	urn:...:p20:user.p20Uid	Unified Login (Unique Identifier)	policeIdentifierName	p20_uid	String-36	T-36-15-15-101-157974135	
TN-Kennung*	Berechnet	-	-	Participant	o	idp	String-20	BK	Automatisiert gefüllt gemäß Bundesländer/Behördenkürzel der angeschlossenen Teilnehmer[4]
Identitätsstatus	Vorhanden	polizeiAktiv	active	Identity Status	-	-	Boolean	(true/false) oder (0,1)	Sperrt den Benutzer für alle Anwendungen, die ans F-IAM angebunden sind

4 https://confluence.bka.extrapol.de/pages/viewpage.action?pageId=123880492