Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNISCHES

Leitfaden zu den Attributen für Identitätsanbieter (IdP)

10.9.2020 – Version 1.2.1

Föderation der Identitätsdienste im Bildungsraum Schweiz
Fédération des services d'identité de l'espace suisse de formation
Federazione dei servizi di identità nello spazio formativo svizzero
Federaziun dals servetschs d'identitad en il spazi da furmaziun svizzer

1. Ziel des Dokuments

Damit die Föderation der Identitätsdienste als Broker zwischen den Dienstleistungsanbietern (SP) und Identitätsanbietern (IdP) fungieren kann, benötigt es einer gemeinsamen Schnittstelle zwischen diesen beiden Akteuren der Föderation: Die Dienstleistungsanbieter müssen wissen, welche Daten einer Identität sie verlangen dürfen und in welcher Form sie diese erhalten. Gleichzeitig müssen Identitätsdienste wissen, welche Attribute ihrer Identitäten notwendig sind, um einen Dienst eines SP verwenden zu können. Dazu müssen die Attribute, aus denen sich die digitalen Identitäten zusammensetzen, im Verzeichnis der IdP und in einem vordefinierten Format für diese vorhanden sein.

Dieser Leitfaden hilft den IdP, die Edulog beitreten, ihre digitalen Identitäten mit den Attributen anzupassen/zu vervollständigen, die von den SP im Rahmen des Betriebs der Föderation verlangt werden können. Einige dieser Attribute sind sicherlich bereits in den Verzeichnissystemen vorhanden, andere werden interne Änderungen erfordern. Ist beispielsweise ein Attribut im Verzeichnis des betreffenden IdP nicht vorhanden, muss der IdP sein Verzeichnisschema ändern, um es aufzunehmen, und dann die erforderlichen Datenwerte von Identitätsverwaltungen (bspw. Schulverwaltungslösungen) sammeln, um es zu vervollständigen.

Jeder SP wird in der Lage sein, eine Teilmenge von Attributen aus der Gesamtliste anzufordern, abhängig davon, was sein Dienst zum ordnungsgemässen Funktionieren benötigt.

2. Ausschlussregeln und Attributfilterung durch die Föderation

Ausschlussregeln zwischen den Attributen sind möglich: einige Attribute sind spezifisch für Schülerinnen und Schüler, andere nur für Erwachsene, Lehrpersonen oder andere Rollen. Für jedes der Attribute wird dies angegeben. Wenn ein IdP Werte in Attribute einführt, die nicht notwendig sind – z. B. Zyklus für einen Lehrer – kann der Wert des Attributs von der Föderation gefiltert und nicht an den SP weitergegeben werden. Dies ist z. B. beim Geburtsdatum der Fall, das in ein Attribut umgewandelt wird, welches nur das Geburtsjahr angibt.

Ein leerer Wert in einem Attribut wird von der Föderation als "unbekannt" behandelt. Wenn dieses Attribut für den Zugriff auf bestimmte Ressourcen des SP obligatorisch ist, wird der Zugriff nicht gewährt.

3. Verwendung

Das in den folgenden Tabellen dargestellte Feld «Attribut» ist der Name, der zur Beschreibung der von den IdP zu liefernden Werten verwendet wird. Jedes der untenstehenden Attribute kann spezielle Regeln für die Verwendung – z. B. nur für Erwachsene anwendbar – oder Ausschlussregeln bezüglich nutzbarer Werte enthalten.

3.1 Anwendbarkeit

Für die Anwendbarkeit des Attributs auf den Personentyp wird eine visuelle Markierung definiert. Unterschieden wird zwischen Nicht-Lernenden (also notwendigerweise Erwachsene) und Schülerinnen und Schüler (die normalerweise, aber nicht unbedingt, minderjährig sind).

Attribut nur für Nicht-Lernende. Zum Beispiel: Lehrpersonen, Verwaltungsangestellte, ...

Attribut nur für Schülerinnen und Schüler

4. SAML Konfiguration

4.1 Format der Attribute

Die Föderation verwendet standardmässig das SAML-Attributprofil "basic", wie in https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf unter Punkt 4.4.3 definiert.

Das Profil verwendet das Element `<saml:Attribute NameFormat="">` in der SAML-Assertion wie folgt:

`urn:oasis:names:tc:SAML:2.0:attrname-format:basic`

Wie die Form von Attributen in einer SAML-Assertion aussieht, zeigt das folgende Beispiel:

```
<saml:AttributeStatement>
   <saml:Attribute Name="uid"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <saml:AttributeValue xsi:type="xs:string">myuid</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="mail"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <saml:AttributeValue xsi:type="xs:string">myuid@testidp.ch</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="EdulogPersonRole"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <saml:AttributeValue xsi:type="xs:string">teacher</saml:AttributeValue>
         <saml:AttributeValue xsi:type="xs:string">principal</saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

Die OID der Attribute werden in diesem Leitfaden zu Informationszwecken bereitgestellt. Wenn sie dennoch bei der Erstellung der Attribute eingesetzt werden müssen (z. B. in der Schemaerweiterung eines Microsoft Active Directory), sollten sie verwendet werden.

4.2 Attribute mit mehreren Werten

Das Beispiel des <AttributeStatement> oben zeigt den Fall des Attributs *EdulogPersonRole*, dessen Multiplizität «mehrere» ist. Hier hat die Identität zwei Rollen im IdP: *teacher* und *principal*.

Die Föderation Edulog unterstützt zwei Formen der Attributübergabe:

1) Wie im Beispiel oben angegeben. Für jeden Wert eines mehrwertigen Attributs wird ein `<saml:AttributeValue ...>` übergeben. Wenn möglich, sollten mehrwertige Attribute mit dieser Syntax übergeben werden.

2) Ein einzelner `<saml:AttributValue ...>` mit mehreren Werten, die durch eine vordefinierte Trennzeichenfolge getrennt sind: ##

Ein Beispiel dafür wäre:

```
<saml:AttributeValue xsi:type="xs:string">teacher##principal</saml:AttributeValue>
```

Diese zweite Version ist für einige IdP-Produkte erforderlich, die Version 1) der Übergabe mehrwertiger Attribute (noch) nicht unterstützen (z. B. *Azure AD*).

Solche IdP müssen daher OBLIGATORISCH mehrere Werte in ihrem Verzeichnis mit der Zeichenkette ## trennen.

z. B.: Für EdulogPersonLevel: secondary1##secondary2##primary

Stellen Sie sicher, dass, wenn nur ein Wert in einem mehrwertigen Attribut vorhanden ist, die vordefinierte Trennzeichenfolge nicht vorhanden ist.

4.3 NameID

Das Element <NameID> wird in SAML 2.0 verwendet, um das Subjekt der SAML-Assertion zu identifizieren, die von der Föderation an den IdP und vom IdP an die Föderation übermittelt wird. Es ist notwendig, dass das Element <NameID> die eindeutige Kennung dieses Subjekts (die uid) in seinem IdP ist.

Falls die uid innerhalb des IdP als username/UPN/samAccountName verwendet wird (d. h. uid=username), läuft der Login-Prozess wie folgt ab: Der Benutzer gibt sein Pseudonym auf Edulog ein. Die uid wird anschliessend im SAML-Request and den IdP gesendet.

Für den Fall «uid=username» muss man jedoch folgendes beachten: Wenn sich der Benutzername im IdP ändert (z. B. aufgrund einer Heirat), muss die Identität der Person defödériert und schliesslich über die API-Funktion der Föderation erneut föderiert werden.

Die andere Möglichkeit ist, eine uid zu verwenden, die sich vom username unterscheidet, aber eindeutig ist (z. B. uid=*ObjectID* in *Azure*, die unabhängig vom username oder der E-Mail-Adresse ist). In diesem Fall könnte die Authentifizierung auf der IdP-Seite betroffen sein, und der Benutzer muss seinen username erneut eingeben, um sich in seinem IdP zu authentifizieren.

4.4 Liste der Attribute

In der folgenden Liste sind alle im folgenden Absatz aufgeführten Attribute aufgeführt. DAS ANGEGEBENE FORMAT DER ATTRIBUTE MUSS ZWINGEND EINGEHALTEN WERDEN (GROSS- UND KLEINSCHREIBUNG EINGESCHLOSSEN).

SAML attribute name
givenName
sn
EdulogPersonBirthDate
preferredLanguage
EdulogPersonRole
mail
o
EdulogPersonLevel
EdulogPersonCycle
EdulogPersonCanton
title
EdulogPersonTechID
uid

5. Attribute für Edulog

Die Liste der für einen IdP erforderlichen Attribute lautet wie folgt:

5.1 Vorname

SAML attribute name	givenName
Beschreibung	Vorname(n) der Person
Anwendbar für	 
OID (informational)	2.5.4.42
Beispiele	Peter Sarah Katherine
Erlaubte Werte	Alle Darf nicht leer gelassen werden
SQL Datentyp	VARCHAR(255)
LDAP Syntax	Directory String
Multiplizität	einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

5.2 Name

SAML attribute name	sn
Beschreibung	Nachname/Familienname der Person
Anwendbar für	 
OID (informational)	2.5.4.4
Beispiele	Muster Schmidt-Müller Dupont Morand
Erlaubte Werte	Alle Darf nicht leer gelassen werden
SQL Datentyp	VARCHAR(255)
LDAP Syntax	Directory String
Multiplizität	einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentar: Darf nicht leer gelassen werden, kann sich aber – z. B. nach einer Heirat oder Adoption – verändern.

5.3 Geburtsdatum

SAML attribute name	EdulogPersonBirthDate
Beschreibung	Geburtsdatum der Person
Anwendbar für	
OID (informational)	1.3.6.1.4.1.38688.1.1.1.3
Beispiele	20030424 *empty*
Erlaubte Werte	*date-mday* MUSS innerhalb des richtigen Bereichs liegen, abhängig von den Werten von *date-month* und *date-fullyear*
SQL Datentyp	VARCHAR(8)
LDAP Syntax	Numeric String{8}
Multiplizität	Einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentar: Dieses Attribut ist für Schülerinnen und Schüler wichtiger als für Lehrpersonen (Erwachsene). Es erlaubt, das Alter zu kontrollieren und eine Altersklasse davon abzuleiten. Einige SP müssen rechtliche Beschränkungen hinsichtlich des Zugangs von Minderjährigen zu ihren Diensten beachten. Fehlt ein Wert in diesem Feld bei einer minderjährigen Person (erkannt durch das Attribut *EdulogPersonRole*), wird die Person standardmässig als minderjährig im niedrigsten Altersrang behandelt, d. h. < 6 Jahre alt (vgl. Attribut für SP, *EdulogPersonAgeCategory*)

Syntax: Basiert auf «Date and Time on the Internet: Timestamps (RFC3339)». Verwendet wird das 'full-date'-Format aus Absatz 5.6, aber **ohne die Bindestriche** zwischen den verschiedenen Teilen:

full-date	=date-fullyeardate-monthdate-mday
date-fullyear	=4DIGIT
date-month	=2DIGIT;01-12
date-mday	=2DIGIT;01-28,01-29,01-30,01-31 based on month/year

5.4 Sprache

SAML attribute name	preferredLanguage
Beschreibung	Die primäre Kommunikationssprache der Person
Anwendbar für	 
OID (informational)	2.16.840.1.113730.3.1.39
Beispiele	de-CH it-CH en
Erlaubte Werte	Nur die folgenden Werte sind zulässig: • *de*-CH • *fr*-CH • *it*-CH • *rm*-CH • *en* Dieses Feld darf leer gelassen werden
SQL Datentyp	ENUM<...>
LDAP Syntax	Directory String
Multiplizität	einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentar: Wenn der Wert nicht vom IdP bereitgestellt wird, bestimmt die Föderation den Wert entsprechend der Kantonssprache. Wenn der Kanton zweisprachig ist, ist dies die Sprache, die in diesem Kanton am meisten gesprochen wird. Kann für die Sprachauswahl in Anwendungen verwendet werden.

Syntax: In Anlehnung an «Tags for Identifying Languages (RFC5646)»

5.5 Rolle

SAML attribute name	EdulogPersonRole
Beschreibung	Hauptrolle der Person
Anwendbar für	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.2
Beispiele	pupil teacher, principal, technician other *empty*
Erlaubte Werte	Nur die folgenden Werte sind zulässig: • *pupil* • *teacher* • *administration* • *principal* • *legal_guardian* • *technician* • *other* Dieses Feld darf leer gelassen werden. **Es wird jedoch dringend empfohlen, es auszufüllen.**
SQL Datentyp	ENUM<...>
LDAP Syntax	Directory String
Multiplizität	mehrere

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Beschreibung der Werte:

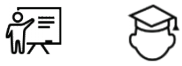
- *empty* (*leer gelassenes Feld*): Die Rolle der Identität in der Bildungseinrichtung ist unbekannt. Wenn dieser Wert verwendet wird, wird die Föderation ihn nicht durch einen Standardwert ersetzen, um zu vermeiden, dass eine falsche Rolle zugewiesen wird. Keine Angabe in diesem Feld kann bedeuten, dass der Zugang zu einem Dienst extrem eingeschränkt, wenn nicht gar unmöglich wird. Es wird dringend empfohlen, die Rolle(n) der Person einzutragen.
- *pupil*: Schülerin/Schüler. Kann nicht in Verbindung mit einem anderen Wert kumuliert werden: einzigartig.
- *teacher*: Lehrperson. Kann in Verbindung mit folgenden Werten verwendet werden: *administration, principal, technician*.
- *administration*: Rolle im Zusammenhang mit der Schulverwaltung, aber nicht mit dem Unterricht. Auch ein Lehrer kann diese Rolle innehaben.
- *principal*: Rolle der Schulleitung. Vielleicht auch eine Lehrperson. Kann nicht kombiniert werden mit *administration*.

- *legal_guardian*: die erziehungsberechtigte Autorität eines Kindes im Sinne des Zivilgesetzbuches. In der Regel die Eltern, der Betreuer, der Vormund. Nur wenn diese im IdP aufgenommen wurden.
- *technician*: technische Rolle in der Schule, z. B. IT-Manager, Sprachtherapeut, Instandhaltung. Kann mit der Position einer Lehrperson kombiniert werden.
- *other*: andere Stellen in einer Bildungseinrichtung, die nicht mit pädagogischen, administrativen oder technischen Aufgaben verbunden sind, z. B. Reinigung. Nicht unbedingt in einem IdP vorhanden, z. B. wenn die Person keinen Zugang zu Anwendungen hat.

Syntax:

- Wenn *empty, other, pupil* oder *legal_guardian* ausgewählt wird, kann es nicht mit anderen Werten kumuliert werden.
- *teacher, administration, principal, technician*: Sind kumulierbar. Ausnahme: *administration* und *principal* sind nicht kumulativ.
- Wenn eine der Rollen ausreicht, um auf einen angeforderten Dienst zuzugreifen, wird sie verwendet. Wenn mehr als eine Rolle vorhanden ist, prüft der SP die Rolle mit den Zugangsbedingungen zum Dienst – z. B. kann die Rolle *administration* den Zugang zu Diensten erlauben, die für eine Lehrperson nicht zugänglich sind.
- Wenn der IdP nicht mehrere Werte überträgt, die jeweils durch ein `<saml:AttributeValue ...>` getrennt sind (siehe Abschnitt 4.2) – z. B. im Fall von *Azure AD* – ist es OBLIGATORISCH, dass die Werte im SAML-Token durch die vordefinierte Trennzeichenfolge getrennt werden: ##
  Beispiel: teacher##principal##technician

5.6 E-Mail-Adresse

SAML attribute name	mail
Beschreibung	E-Mail-Adresse der Person
Anwendbar für	
OID (informational)	0.9.2342.19200300.100.1.3
Beispiele	peter.muster@institution.kanton.ch
Erlaubte Werte	Alle, solange sie RFC4524 folgen
SQL Datentyp	VARCHAR(255)
LDAP Syntax	IA5 String {256}
Multiplizität	einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Syntax: Gemäss «COSINE LDAP/X.500 Schema (RFC4524)» – Es gilt zu beachten, dass E-Mail-Adressen im Unterschied zu RFC4524 einzigartig sind. Gemeint ist die berufliche/schulische E-Mail-Adresse.

5.7 Institution

SAML attribute name	o
Beschreibung	Name der Institution(en), in der/denen sich die Person befindet
Anwendbar für	 
OID (informational)	2.5.4.10
Beispiele	Gymnase de Beaulieu Martigny EP, Lycée Jean-Piaget *empty*
Erlaubte Werte	Alle Kann leer gelassen werden
SQL Datentyp	VARCHAR(255)
LDAP Syntax	Directory String
Multiplizität	Mehrere

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentare: Es ist zu beachten, dass häufig Kürzel verwendet werden (z. B. GIBB). Weiter ist zu beachten, dass es bei Lehrpersonen relativ häufig «mehrere» sein kann.

Syntax: Wenn der IdP nicht mehrere Werte überträgt, die jeweils durch ein `<saml:AttributeValue ...>` getrennt sind (siehe Abschnitt 4.2) – z. B. im Fall von *Azure AD* – ist es OBLIGATORISCH, dass die Werte im SAML-Token durch die vordefinierte Trennzeichenfolge getrennt werden: ##
Beispiel: Martigny EP##Lycée Jean-Piaget

5.8 Bildungsstufe

SAML attribute name	EdulogPersonLevel
Beschreibung	Bildungsstufe einer Schülerin/eines Schülers Im Falle einer Lehrperson die Hauptstufe(n), auf der/denen er/sie unterrichtet
Anwendbar für	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.4
Beispiele	primary primary, secondary1 *empty*
Erlaubte Werte	• *primary* • *secondary1* • *secondary2* • *tertiary* Kann leer gelassen werden
SQL Datentyp	VARCHAR(255)
LDAP Syntax	Directory String
Multiplizität	Mehrere

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Syntax: Wenn der IdP nicht mehrere Werte überträgt, die jeweils durch ein `<saml:AttributeValue ...>` getrennt sind (siehe Abschnitt 4.2) – z. B. im Fall von *Azure AD* – ist es OBLIGATORISCH, dass die Werte im SAML-Token durch die vordefinierte Trennzeichenfolge getrennt werden: ##
Beispiel: primary##secondary1##secondary2

5.9 Zyklus

SAML attribute name	EdulogPersonCycle
Beschreibung	Bildungszyklus einer Schülerin/eines Schülers Im Falle einer Lehrperson der Zyklus/die Zyklen, in dem/denen in dem/denen die Person hauptsächlich unterrichtet
Anwendbar für	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.5
Beispiele	1 *empty* 0 1, 2
Erlaubte Werte	• *0 (not applicable)* • *1 (cycle1)* • *2 (cycle2)* • *3 (cycle3)* Kann leer gelassen werden
SQL Datentyp	ENUM <...>
LDAP Syntax	Directory String
Multiplizität	Mehrere

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentar: Die verschiedenen Zyklen sind in den jeweiligen Lehrplänen (PER, Lehrplan 21, TI) beschrieben, siehe hierzu: https://edudoc.ch/record/111988/files/schuleintritt_d.pdf

Syntax:

- *0* = nicht zutreffend: für Fälle, in denen bekannt ist, dass die Person weder innerhalb des entsprechenden Zyklus unterrichtet wird noch in diesem arbeitet (z. B. ein Schüler der Sekundarstufe II oder ein Techniker).
- *empty* = Die Situation der Person ist nicht bekannt.
- Wenn der IdP nicht mehrere Werte überträgt, die jeweils durch ein `<saml:AttributeValue ...>` getrennt sind (siehe Abschnitt 4.2) – z. B. im Fall von *Azure AD* – ist es OBLIGATORISCH, dass die Werte im SAML-Token durch die vordefinierte Trennzeichenfolge getrennt werden: ##
  Beispiel: 0##1

5.10 Kanton

SAML attribute name	EdulogPersonCanton
Beschreibung	Kanton, zu dem der IdP der betreffenden Person gehört
Anwendbar für	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.6
Beispiele	VD ZH FL XX *empty*
Erlaubte Werte	• *ZH* • *BE* • *LU* • ... • *FL* • *XX*
SQL Datentyp	ENUM<...>
LDAP Syntax	Directory String
Multiplizität	einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentar: Abkürzung des Kantons (gemäss Art. 84 der Verkehrszulassungsverordnung VZV), der für die betreffende Identität zuständig ist. Wenn es aus irgendeinem Grund nicht möglich ist, zu wissen, zu welchem Kanton die Identität gehört, wird dieser Wert auf *empty* gesetzt. Sonderfall für Schulen im Ausland, die zwar von einem Kanton abhängen, aber möglicherweise ausländischem Recht unterliegen.

Syntax: Abkürzungen nach Art. 84 des VZV

- *FL*: für das Fürstentum Liechtenstein.
- *XX*: entspricht einem nicht-schweizerischen Gebiet (z. B. eine Schweizer Schule in Mexiko).

5.11 Funktion

SAML attribute name	title
Beschreibung	Stellenbezeichnung, die frei gewählt werden kann Gilt nicht für Lernende
Anwendbar für	
OID (informational)	2.5.4.12
Beispiele	IT-Administrator Logopädin Sekretariat *empty*
Erlaubte Werte	Alle Kann leer gelassen werden
SQL Datentyp	VARCHAR(255)
LDAP Syntax	Directory String
Multiplizität	einzigartig

Ausschlussregeln: Gilt nicht für Lernende.

Syntax: Jeder IdP muss die verschiedenen Klassen von Funktionen innerhalb seines Geltungsbereichs identifizieren. Die Funktionen sind nicht unbedingt mit denen anderer Kantone/IdP vergleichbar.

5.12 Technischer Identifikator

SAML attribute name	EdulogPersonTechID
Beschreibung	Eine eindeutige Kennung, die von der Föderation generiert und bereitgestellt wurde und die vom Benutzer nie geändert werden kann.
Anwendbar für	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.1
Beispiele	110e8400-e29b-11d4-a716-446655440000
Erlaubte Werte	Darf nicht leer gelassen werden
SQL Datentyp	VARCHAR(36)
LDAP Syntax	Directory String
Multiplizität	einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Kommentar: Eine eindeutige Kennung, die von der Föderation generiert und bereitgestellt wurde und die vom Benutzer nie geändert werden kann.

5.13 Identitätsanbieter-Identifikation

SAML attribute name	uid
Beschreibung	Eine eindeutige Kennung für eine Person, die zur Identifizierung des Benutzers in deren IdP verwendet wird, von dem sie abhängt.
Anwendbar für	
OID (informational)	0.9.2342.19200300.100.1.1
Beispiele	peter.muster@institution.kanton.ch
Erlaubte Werte	Bestimmt durch den IdP. Darf nicht leer gelassen werden
SQL Datentyp	VARCHAR(255)
LDAP Syntax	Directory String
Multiplizität	Einzigartig

Ausschlussregeln: Keine. Alle Identitäten sind einbezogen.

Syntax: Wird vom IdP bestimmt. Muss mit dem angegebenen LDAP-Format kompatibel sein, muss EINZIGARTIG sein und darf sich im Verzeichnis des IdP nicht ändern.

Wenn der IdP auf einem Microsoft AD basiert, kann er die Werte des UPN-Attributs (*UserPersonalName*) vorrangig oder das *samAccountName*-Attribut verwenden. Wie angegeben, darf sich die Identifikation innerhalb des IdP nicht ändern.

Wenn uid=username (oder =*UserPersonalName* oder =*samAccountName*) und sich diese ändert (z. B. infolge einer Heirat), dann muss die Identität defödériert und neu föderiert werden, damit Edulog die Eindeutigkeit der Identität aufrechterhalten kann.

Wenn uid<>username (oder *UserPersonalName* oder *samAccountName*) und er sich im Laufe der Zeit nicht ändern kann oder ändert (z. B. *Azure ObjectID*), dann ist es nicht notwendig erneut zu föderieren, falls sich der username ändert. Dies kann jedoch zu Problemen der Authentifizierung beim IdP führen.

Versionenkontrolle

Datum	Version	Änderungen
10.9.2020	1.2.1	Klarstellung in 5.3 (EdulogPersonBirthDate) bezüglich des Fehlens von Bindestrichen im Abschnitt «Syntax». Erstellung «Versionenkontrolle»