Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Berne

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

Guide des attributs pour des fournisseurs d'identité (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. But du document

Pour que la fédération d'identité puisse servir de broker entre les fournisseurs de services (SP) et les fournisseurs d'identité (IdP), il faut qu'il existe une interface commune entre tous les acteurs de la fédération : les SP doivent savoir quelles sont les données d'une identité qu'ils peuvent demander et dans quel format les recevoir. De même, les IdP doivent savoir quels attributs de ses identités sont nécessaires pour pouvoir utiliser un service d'un SP. Pour cela les attributs qui composent les identités numériques doivent être présents dans l'annuaire des IdP et un format pour ceux-ci prédéfini.

Ce guide aide les IdP rejoignant Edulog à adapter/compléter leurs identités numériques avec les attributs que les SP pourraient demander dans le cadre de l'exploitation de la Fédération. Certains de ces attributs sont sûrement déjà présents dans les systèmes d'annuaires, d'autres nécessiteront de modifications internes. Ainsi, si un attribut n'existe pas dans l'annuaire du IdP considéré, il faut que celui-ci modifie le schéma de son annuaire pour l'incorporer et ensuite recueillir les valeurs nécessaires des données auprès des gestionnaires des identités (par ex. solutions pour l'administration scolaire) pour les compléter.

Chaque SP pourra demander un sous-ensemble d'attributs de la liste complète, dépendant de ce dont leur service a besoin pour fonctionner correctement.

2. Règles d'exclusions et filtrage des attributs par la fédération

Des règles d'exclusion entre attributs sont possibles : certains attributs sont spécifiques aux élèves, d'autres uniquement à des adultes, enseignants ou autres rôles. Pour chacun des attributs cela est spécifié. Si un IdP introduit des valeurs dans des attributs qui ne sont pas nécessaires – exemple : le cycle pour un enseignant – la valeur de l'attribut pourra être filtré par la fédération et ne pas être fourni au SP. Ce sera le cas par exemple, de la date de naissance, qui sera transformée dans un attribut qui uniquement donnera l'année de naissance.

Une valeur vide dans un attribut est traitée comme « inconnue » par la Fédération. Si cet attribut est obligatoire pour l'accès à certaines ressources du SP, l'accès n'est pas accordé.

3. Utilisation

Le champ « attribut » indiqué dans les tables suivantes, sera le nom utilisé pour décrire les valeurs qui doivent être fournies par les IdP. Chacun des attributs ci-dessous peut avoir des règles particulières d'utilisation – par ex. : applicable uniquement aux adultes – ou des règles d'exclusions concernant les valeurs utilisables.

3.1 Applicabilité

On définit un marqueur visuel pour l'applicabilité de l'attribut au type de personne. On sépare entre non-élèves (donc forcément adultes) et élèves (qui sont généralement mineurs, mais pas forcément).

Attribut uniquement pour non-élèves. Par exemple : enseignants, administratifs, ...

Attribut uniquement pour élèves.

4. Configuration de SAML

4.1 Format des attributs

La fédération utilise par défaut le SAML Attribute Profile « basic », tel que définit dans https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf au point 4.4.3.

Le profil utilise l'élément `<saml:Attribute NameFormat="">` dans l'assertion SAML, tel que :

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

Un exemple de représentation des attributs dans une assertion est de la forme suivante :

```
<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>
```

Les OID des attributs sont fournis dans ce guide dans un but d'information. Néanmoins, si ceux-ci doivent être utilisés lors de la création des attributs (par exemple, dans l'extension du schéma d'un Active Directory de Microsoft), on doit les utiliser.

4.2 Attributs avec valeurs multiples

L'exemple d' < AttributeStatement > ci-dessus montre le cas de l'attribut *EdulogPersonRole* dont la multiplicité est « multiple ». Ici, l'identité possède deux rôles dans l'IdP : *teacher* et *principal*.

La fédération Edulog, supporte deux formes de passage des attributs :

1) Celle de l'exemple. Pour chaque valeur d'un attribut multi-valué, un `<saml:AttributeValue ...>` est passé. Si possible, les attributs multi-valués doivent être transmis via cette syntaxe.

2) Un unique `<saml:AttributValue ...>` avec plusieurs valeurs séparées par une chaine de caractères de séparation prédéfini : ##

Ainsi un exemple serait :

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

Cette deuxième version est nécessaire pour certains produits IdP qui ne supportent pas (encore) la version 1) de passage d'attributs multi-valués (ex : *Azure AD*).

Ces IdP doivent donc OBLIGATOIREMENT séparer les valeurs multiples dans leur directory avec la chaîne ##

ex. : Pour EdulogPersonLevel : secondary1##secondary2##primary

A noter, que s'il n'y a qu'une seule valeur dans un attribut multi-valué, la chaîne de caractères réservée n'est pas présente.

4.3 NameID

L'élément <NameID> est utilisé dans SAML 2.0 pour identifier le sujet de l'assertion SAML transmise par la fédération vers l'IdP et depuis l'IdP vers la fédération. Il faut que l'élément <NameID> soit l'identifiant unique de ce sujet (l'uid) dans son IdP.

Si l'uid est utilisé dans l'IdP comme username/UPN/samAccountName (c.a.d. uid=username), le processus de connexion se déroule comme suit : l'utilisateur saisit son pseudonyme sur Edulog. L'uid est ensuite envoyé à l'IdP dans la requête SAML.

Pour le cas 'uid=nom d'utilisateur', il faut cependant respecter les points suivants : Si le nom d'utilisateur change dans l'IdP (par exemple en raison d'un mariage), l'identité de la personne doit être défédérée et finalement fédérée à nouveau à travers la fonction API de la Fédération.

L'autre option est d'utiliser un uid qui soit différent du username, mais unique (ex : uid=ObjectID dans *Azure*, qui est indépendant du username ou de l'email). Dans ce cas, l'authentification du côté de l'IdP pourrait être affecté et l'utilisateur devra réintroduire son username pour s'authentifier dans son IdP.

4.4 Liste des attributs

La liste suivante recueille tous les attributs spécifiés dans les pages suivants. LE FORMAT SPÉCIFIÉ DES ATTRIBUTS DOIT ÊTRE RESPECTÉ (MAJUSCULES ET MINUSCULES INCLUSES).

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

5.

6. Attributs pour Edulog

La liste des attributs nécessaires pour un IdP est la suivante :

6.1 prénom

SAML attribute name	givenName
Description	Prénom(s) de la personne
Applicable aux	 
OID (informational)	2.5.4.42
Exemples	Peter Sarah Katherine
Valeurs permises	Toutes Ne peut être vide
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	Directory String
Multiplicité	unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

6.2 nom

SAML attribute name	sn
Description	Nom de famille de la personne
Applicable aux	 
OID (informational)	2.5.4.4
Exemples	Muster Schmidt-Müller Dupont Morand
Valeurs permises	Toutes Ne peut être vide
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	Directory String
Multiplicité	unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaire : ne peut être vide, mais peut changer – par ex. : après mariage ou adoption.

6.3 date de naissance

SAML attribute name	EdulogPersonBirthDate
Description	Date de naissance de la personne
Applicable aux	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.3
Exemples	20030424 *empty*
Valeurs permises	*date-mday* DOIT se situer dans la limite appropriée en fonction des valeurs de *date-month* and *date-fullyear*
Type de données SQL	VARCHAR(8)
Syntaxe LDAP	Numeric String{8}
Multiplicité	unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaire : Cet attribut est plus important pour les enfants que pour les adultes. Il permet de contrôler l'âge et dériver après une classe d'âge pour celui-ci. Certains SP doivent respecter des contraintes légales concernant l'accès de mineurs à leurs services. Pour un mineur (identifié par son attribut *EdulogPersonRole*) l'absence de valeur dans ce champ sera traitée, par défaut, comme celui d'étant un mineur dans le rang d'âge le plus bas, c.a.d. : < 6ans (cf. attribut pour les SP, *EdulogPersonAgeCategory*).

Syntaxe : Basée sur « Date and Time on the Internet: Timestamps (RFC3339) » en utilisant le 'full-date' format du paragraphe 5.6, mais sans les tirets entre les différentes parties :

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

6.4 langue

SAML attribute name	preferredLanguage
Description	Langue préférée de la personne
Applicable aux	
OID (informational)	2.16.840.1.113730.3.1.39
Exemples	de-CH it-CH en
Valeurs permises	Sont uniquement permises les valeurs suivantes : • *de*-CH • *fr*-CH • *it*-CH • *rm*-CH • *en* Ce champ peut être vide
Type de données SQL	ENUM<...>
Syntaxe LDAP	Directory String
Multiplicité	unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaire : Dans le cas où la valeur n'est pas fournie par le IdP, la Fédération déterminera la valeur en fonction de la langue cantonale. Si le canton est bilingue, ce sera la langue la plus parlée dans ce canton. Pourra être utilisé pour la sélection de la langue dans les applications.

Syntaxe : Suivant « Tags for Identifying Languages (RFC5646) »

6.5 rôle

SAML attribute name	EdulogPersonRole
Description	Rôle principal de la personne
Applicable aux	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.2
Exemples	pupil teacher, principal, technician other *empty*
Valeurs permises	Seules les valeurs suivantes sont permises : • *pupil* • *teacher* • *administration* • *principal* • *legal_guardian* • *technician* • *other* Ce champ peut être vide. **Il est néanmoins fortement recommandé de le remplir.**
Type de données SQL	ENUM<...>
Syntaxe LDAP	Directory String
Multiplicité	multiple

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Description des valeurs :

- *empty* (champ vide) : Le rôle de l'identité dans l'institution scolaire est inconnu. Si cette valeur est utilisée la fédération ne la remplacera pas par une valeur par défaut, pour éviter des supplantations. L'absence d'entrée dans ce champ peut signifier que l'accès à un service devient extrêmement limité, voire impossible. Il est fortement recommandé d'indiquer le(s) rôle(s) de la personne.
- *pupil* : élève. Ne peut être utilisé en même temps qu'une autre valeur : valeur unique.
- *teacher* : enseignant. Peut-être cumulé avec les valeurs suivantes : *administration*, *principal*, *technician*.
- *administration* : rôle lié à l'administration de l'école mais pas à l'enseignement. Un enseignant peut aussi cumuler ce rôle.
- *principal* : rôle de direction de l'école. Peut-être aussi un enseignant. Non cumulable avec administration.
- *legal_guardian* : responsable de l'autorité parentale d'un enfant au sens du code civil. Généralement les parents, tuteur, curateur. Seulement si ceux-ci sont inclus dans l'IdP.

- *technician* : rôle technique de l'établissement scolaire, par exemple : responsable informatique, logopède, maintenance. Peut-être cumulé avec le poste d'un enseignant.
- *other* : autres postes d'un établissement scolaire non lié à une fonction enseignante, administrative ou technique, par exemple : nettoyage. Pas nécessairement présent dans un IdP si ne possède pas d'accès à des applications.

Syntaxe :

- Si *empty*, *other*, *pupil* ou *legal_guardian* sont sélectionnés, alors il ne peut pas être cumulé avec d'autres valeurs.
- *teacher*, *administration*, *principal*, *technician*. Peuvent se cumuler. Exception : *administration* et *principal* ne le sont pas entre eux.
- Si un des rôles est suffisant pour accéder au service demandé, celui-ci sera utilisé. Si plusieurs sont présents, le SP vérifiera le rôle avec les conditions d'accès au service – par ex. : la rôle administration permet d'accéder à des services non accessibles à un enseignant.
- Si l'IdP ne transmet pas des valeurs multiples séparées chacune par un `<saml:AttributeValue ...>` (voir paragraphe 4.2) – cas d'*Azure AD*, par exemple –, il faut OBLIGATOIREMENT que les valeurs soient séparées dans le jeton SAML par la chaîne de caractères réservée : ##
  Exemple : teacher##principal##technician

6.6 courriel

SAML attribute name	mail
Description	adresse électronique principale de la personne
Applicable aux	
OID (informational)	0.9.2342.19200300.100.1.3
Exemples	peter.muster@institution.canton.ch
Valeurs permises	Toutes, si elles suivent RFC4524
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	IA5 String {256}
Multiplicité	unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Syntaxe : Suivant « COSINE LDAP/X.500 Schema (RFC4524) » – à noter qu'à différence de RFC4524, l'adresse électronique est unique. Il s'agit ici de l'adresse électronique professionnelle.

6.7 établissement

SAML attribute name	o
Description	Nom de/des l'établissement/s d'appartenance de la personne
Applicable aux	 
OID (informational)	2.5.4.10
Exemples	Gymnase de Beaulieu Martigny EP, Lycée Jean-Piaget *empty*
Valeurs permises	Toutes Peut être vide
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	Directory String
Multiplicité	Multiple

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaires : Il convient de noter que des désignations courtes sont souvent utilisées (par exemple GCB). A noter qu'il peut être relativement souvent « multiple » dans le cas des enseignants.

Syntaxe : Si l'IdP ne transmet pas des valeurs multiples séparées chacune par un `<saml:AttributeValue ...>` (voir paragraphe 4.2) – cas d'*Azure AD*, par exemple –, il faut OBLIGATOIREMENT que les valeurs soient séparées dans le jeton SAML par la chaîne de caractères réservée : ##
Exemple : Martigny EP##Lycée Jean-Piaget

6.8 niveau d'enseignement

SAML attribute name	EdulogPersonLevel
Description	Niveau éducatif d'un élève Dans le cas d'un enseignant, niveau(x) dans le(s)quel(s) il enseigne
Applicable aux	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.4
Exemples	primary primary, secondary1 *empty*
Valeurs permises	• *primary* • *secondary1* • *secondary2* • *tertiary* Peut être vide
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	Directory String
Multiplicité	Multiple

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Syntax : Si l'IdP ne transmet pas des valeurs multiples séparées chacune par un `<saml:AttributeValue …>` (voir paragraphe 4.2) – cas d'*Azure AD*, par exemple –, il faut OBLIGATOIREMENT que les valeurs soient séparées dans le jeton SAML par la chaîne de caractères réservée : ##
Exemple : primary##secondary1##secondary2

6.9 cycle

SAML attribute name	EdulogPersonCycle
Description	Cycle éducatif d'un élève Dans le cas d'un enseignant, cycle(s) dans le(s)quel(s) il enseigne
Applicable aux	
OID (informational)	1.3.6.1.4.1.38688.1.1.1.5
Exemples	1 *empty* 0 1, 2
Valeurs permises	• *0 (not applicable)* • *1 (cycle1)* • *2 (cycle2)* • *3 (cycle3)* Peut être vide
Type de données SQL	ENUM <...>
Syntaxe LDAP	Directory String
Multiplicité	Multiple

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaires : Les différents cycles éducatifs sont décrits dans les plans d'études respectifs (PER, Lehrplan21, TI), voir ici : http://edudoc.ch/record/111987/files/schuleintritt_f.pdf.

Syntaxe :

- *0* – non applicable : pour les cas où l'on sait que la personne ne suit ni le cycle correspondant, ou ne travaille pas dans le cycle correspondant (par ex : élève du secondaire II, ou un technicien).
- *Empty :* on ne sait pas quelle est la situation de la personne.
- Si l'IdP ne transmet pas des valeurs multiples séparées chacune par un `<saml:AttributeValue ...>` (voir paragraphe 4.2) – cas d'*Azure AD*, par exemple –, il faut OBLIGATOIREMENT que les valeurs soient séparées dans le jeton SAML par la chaîne de caractères réservée : ##
  Exemple : 0##1

6.10 canton

SAML attribute name	EdulogPersonCanton
Description	Canton d'appartenance de l'IdP de la personne considérée
Applicable aux	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.6
Exemples	VD ZH FL XX *empty*
Valeurs permises	• *ZH* • *BE* • *LU* • ... • *FL* • *XX*
Type de données SQL	ENUM<...>
Syntaxe LDAP	Directory String
Multiplicité	Unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaires : Abréviation du canton (selon l'art. 84 de l'Ordonnance réglant l'admission à la circulation routière OAC), responsable de l'identité considérée. Si, pour une raison quelconque, il n'est pas possible de savoir à quel canton l'identité appartient, cette valeur est fixée à *empty*. Cas particulier des écoles à l'étranger qui, même si elles peuvent dépendre d'un canton, peuvent être soumises à des lois étrangères.

Syntaxe : Abréviations selon l'art. 84 de la OAC – plaques d'immatriculation.

- *FL* : est pour la Principauté de Liechtenstein.
- XX : correspond à un territoire non suisse (par exemple, une école suisse au Méxique).

6.11 fonction

SAML attribute name	title
Description	Titre du poste, qui peut être choisi librement Ne s'applique pas aux élèves
Applicable aux	
OID (informational)	2.5.4.12
Exemples	Administrateur IT Logopède Secrétariat *empty*
Valeurs permises	Toutes Peut être vide
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	Directory String
Multiplicité	Unique

Règles d'exclusion : Ne s'applique pas aux élèves.

Syntaxe : Chaque IdP doit identifier les différentes classes de fonctions dans leur périmètre. Les fonctions ne sont pas forcément assimilables à celles d'autres cantons/IdP.

6.12 identificateur technique

SAML attribute name	EdulogPersonTechID
Description	Un identifiant unique généré et fourni par la Fédération, qui ne peut jamais être modifié par l'utilisateur.
Applicable aux	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.1
Exemples	110e8400-e29b-11d4-a716-446655440000
Valeurs permises	Ne peut être vide
Type de données SQL	VARCHAR(36)
Syntaxe LDAP	Directory String
Multiplicité	Unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Commentaires : Il s'agit d'un identifiant unique généré et fourni par la Fédération et qui ne peut jamais être modifié par l'utilisateur.

6.13 numéro d'identification du fournisseur d'identités

SAML attribute name	uid
Description	Un identifiant unique pour une personne, utilisé pour l'identification de l'utilisateur dans l'IdP duquel il dépend.
Applicable aux	 
OID (informational)	0.9.2342.19200300.100.1.1
Exemples	peter.muster@institution.canton.ch
Valeurs permises	Déterminé par l'IdP Ne peut être vide
Type de données SQL	VARCHAR(255)
Syntaxe LDAP	Directory String
Multiplicité	Unique

Règles d'exclusion : Aucune. Toutes les identités sont concernées.

Syntaxe : Déterminé par l'IdP, doit pouvoir être compatible avec le format LDAP indiqué et doit être UNIQUE.

Si l'IdP est basé sur un Microsoft AD, celui-ci pourra utiliser les valeurs de l'attribut UPN (*UserPersonalName*) en priorité ou celui du *samAccountName*. Comme indiqué il faut que l'identification au sein de l'IdP ne change pas.

Si uid=username (ou =*UserPersonalName* ou =*samAccountName*) et que celui-ci change (par exemple, à la suite d'un mariage), alors l'identité doit être défédérée et refédérée, pour qu'Edulog puisse maintenir l'unicité de l'identité.

Si uid<>username (ou *UserPersonalName* ou *samAccountName*) et qu'il ne peut changer au cours du temps (ex : ObjectID d'*Azure*), alors il n'y aura pas besoin de refédérer dans le cas où l'username change. Néanmoins, cela peut entrainer des problèmes d'authentification chez l'IdP.

Notes de version

Date	Version	Changements
10.9.2020	1.2.1	inclut une clarification au point 5.3 (EdulogPersonBirthDate) concernant l'absence d'emploi de tirets au paragraphe « syntaxe » Création « Notes de version »