Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Berne

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

# Guide des attributs pour des fournisseurs de services (SP)

12.5.2020 –Version 1.1



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'identités 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 SP qui s'adhèrent à Edulog à adapter/compléter leurs applications (et leur logique interne) à utiliser les attributs que les IdP pourraient leur transmettre dans le cadre du fonctionnement de la fédération. Certains de ces attributs sont sûrement déjà utilisés, d'autres non. Mais il faut que les formats des attributs soient les même pour éviter les problèmes d'accès des utilisateurs.

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 qui peuvent être reçues par les SP. 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. SAML Konfiguration

### 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 forme de passage des attributs est celle de l'exemple. Pour chaque valeur d'un attribut multi-valué, un <`saml:AttributeValue` …> est passé.

### 4.3 NameID

L'élément <NameID> utilisé dans SAML 2.0 pour identifier le sujet de l'assertion SAML transmise par la fédération Edulog vers le SP est l'attribut *EdulogPersonTechID* (voir plus loin).

### 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 |
| EdulogPersonAgeCategory |
| preferredLanguage |
| EdulogPersonRole |
| mail |
| o |
| EdulogPersonLevel |
| EdulogPersonCycle |
| EdulogPersonCanton |
| title |
| EdulogPersonTechID |
| EdulogPersonYearOfBirth |

## 5. Attributs pour Edulog

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

### 5.1 prénom

| | |
|---|---|
| SAML attribute name | givenName |
| Description | Prénom(s) de la personne |
| Applicable aux |   |
| OID (informational) | 2.5.4.42 |
| Exemples | Peter<br>Sarah Katherine |
| Valeurs permises | Toutes<br>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.

### 5.2 nom

| | |
|---|---|
| SAML attribute name | sn |
| Description | Nom de famille de la personne |
| Applicable aux |   |
| OID (informational) | 2.5.4.4 |
| Exemples | Muster<br>Schmidt-Müller<br>Dupont Morand |
| Valeurs permises | Toutes<br>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.

### 5.3 catégorie d'âge

| | |
|---|---|
| SAML attribute name | EdulogPersonAgeCategory |
| Description | Rang d'âge de la personne |
| Applicable aux |   |
| OID (informational) | 1.3.6.1.4.1.38688.1.1.1.8 |
| Exemples | 6<br>18 |
| Valeurs permises | • 0 (jusqu'à 6 ans)<br>• 6 (de 6 à 8 ans)<br>• 8 (de 8 à 12 ans)<br>• 12 (de 12 à 14 ans)<br>• 14 (de 14 à16 ans)<br>• 16 (de 16 à 18 ans)<br>• 18 (18 ans et plus)<br><br>Ne peut être vide |
| Type de données SQL | ENUM<...> |
| Syntaxe LDAP | Numeric String{2} |
| Multiplicité | unique |

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

**Commentaire** : Cet attribut est plus important pour les élèves que pour les enseignants (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 traité, 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*).

Pour un adulte, si l'âge n'est pas déterminable par *EdulogPersonBirthDate*, l'attribut *EdulogPersonRole* ou *title* sera pris en compte. La valeur transmise sera alors de 18. Si aucun de ces trois attributs n'a de valeur correspondant à un adulte, la valeur transmise sera 0 (un mineur dans le rang d'âge le plus bas).

### 5.4 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<br>it-CH<br>en |
| Valeurs permises | Sont uniquement permises les valeurs suivantes :<br>• *de*-CH<br>• *fr*-CH<br>• *it*-CH<br>• *rm*-CH<br>• *en*<br><br>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 la « Tags for Identifying Languages (RFC5646) »

### 5.5 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<br>teacher, principal, technician<br>other<br>*empty* |
| Valeurs permises | Seules les valeurs suivantes sont permises :<br>• *pupil*<br>• *teacher*<br>• *administration*<br>• *principal*<br>• *legal_guardian*<br>• *technician*<br>• *other*<br><br>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 :**

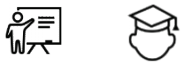
- *empty* (champ vide) : Le rôle de l'identité dans l'institution scolaire est inconnu. Si cette valeur est utilisée la fédération ne la remplacera pas par une valeur par défaut, pour éviter des supplantations. L'absence d'entrée dans ce champ peut signifier que l'accès à un service devient extrêmement 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.

### 5.6 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.

### 5.7 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<br>Martigny EP, Lycée Jean-Piaget<br>*empty* |
| Valeurs permises | Toutes<br>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.

### 5.8 niveau d'enseignement

| | |
|---|---|
| SAML attribute name | EdulogPersonLevel |
| Description | Niveau éducatif d'un élève<br>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<br>primary, secondary1<br>*empty* |
| Valeurs permises | • *primary*<br>• *secondary1*<br>• *secondary2*<br>• *tertiary*<br><br>Peut être vide |
| Type de données SQL | VARCHAR(255) |
| Syntaxe LDAP | Directory String |
| Multiplicité | Multiple |

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

### 5.9 cycle

| | |
|---|---|
| SAML attribute name | EdulogPersonCycle |
| Description | Cycle éducatif d'un élève<br>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<br>*empty*<br>0<br>1, 2 |
| Valeurs permises | • *0 (not applicable)*<br>• *1 (cycle1)*<br>• *2 (cycle2)*<br>• *3 (cycle3)*<br><br>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.

### 5.10 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<br>ZH<br>FL<br>XX<br>*empty* |
| Valeurs permises | • *ZH*<br>• *BE*<br>• *LU*<br>• ...<br>• *FL*<br>• *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).

### 5.11 fonction

| | |
|---|---|
| SAML attribute name | title |
| Description | Titre du poste, qui peut être choisi librement<br>Ne s'applique pas aux élèves |
| Applicable aux |  |
| OID (informational) | 2.5.4.12 |
| Exemples | Administrateur IT<br>Logopède<br>Secrétariat<br>*empty* |
| Valeurs permises | Toutes<br>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.

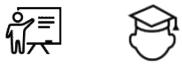
### 5.12 identificateur technique

| | |
|---|---|
| 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.

### 5.13 année de naissance

| | |
|---|---|
| SAML attribute name | EdulogPersonYearOfBirth |
| Description | Année de naissance |
| Applicable aux |  |
| OID (informational) | 1.3.6.1.4.1.38688.1.1.1.7 |
| Exemples | 2009<br>1970<br>*empty* |
| Valeurs permises | à partir de 1900 |
| Type de données SQL | VARCHAR(4) |
| Syntaxe LDAP | Numeric String{4} |
| Multiplicité | unique |

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

**Commentaires :** Cet attribut est plus important pour les élèves que pour les enseignants (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.

La fédération déterminera cet attribut en se basant sur la valeur de l'attribut *EdulogPerson-BirthDate* fournie par l'IdP. En cas d'absence de valeur dans ce champ on regardera la valeur de *EdulogPersonRole*, pour déterminer s'il s'agit d'un adulte ou d'un mineur. S'il s'agit d'un adulte on passera l'année correspondante à 18 ans. Pour un mineur, l'année qui lui donnerait 5 ans.

**Syntaxe :** Basé sur « Date and Time on the Internet: Timestamps (RFC3339) ». Usage du « date-fullyear » format du paragraphe 5.6 : date-fullyear = 4DIGIT