Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

Guide des attributs pour des fournisseurs de services (SP)

5.2023 –Version 1.4

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

Notes de version

Date	Version	Changements
5.2023	1.4	Ajout du chapitre 5 OpenID Connect

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. Attributs SAML

4.1 Format des attributs

La fédération utilise le SAML Attribute Profile «basic», tel que défini 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:At-
         tributeValue>
   </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:At-
         tributeValue>
         <saml:AttributeValue xsi:type="xs:string">principal</saml:At-
         tributeValue>
   </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).

5. Configuration OpenID Connect

5.1 Établir une relation de confiance

Comme pour SAML, l'implémentation d'OpenID Connect (OIDC) nécessite l'établissement préalable d'une relation de confiance (creation of trust) entre l'IdP et Edulog. Pour cela, le SP doit configurer le descripteur OIDC pour Edulog. Les paramètres peuvent être consultés sous les liens suivants :

Intégration: https://go.int.edulog.ch/auth/realms/edulog/.well-known/openid-configuration

Production: https://go.edulog.ch/auth/realms/edulog/.well-known/openid-configuration

5.2 Attributs / Claims

Les attributs sont appelés «Claims» dans OpenID Connect et sont inclus dans le ID Token. Spécificités :

- L'UID doit se trouver dans le claim nommé «sub».
- Les attributs Edulog doivent être contenus dans un claim distinct, comme les autres attributs.
- Les valeurs multiples doivent être fournies dans une table JSON (ou Array).

```
{
  "exp" : 1668693362,
  "iat" : 1668675363,
  "auth_time" : 1668675363,
  "jti" : "7ed997fe-daa9-419c-a15b-6c780548bfac",
  "iss" : "https://go.edulog.ch/auth/realms/edulog",
  "aud" : "...",
  "sub" : <techID>,
  "typ" : "ID",
  "azp" : "...",
  "EdulogPersonRole" : [ "teacher", "principal" ],
  "mail" : "myuid@testidp.ch",
  "uid" : "myuid",
  ...
}
```

Ensuite, le SP envoie son «Client ID» et l'URL de la redirection (Redirect) à Edulog. Edulog configure les paramètres et attributs fournis de son côté et communique au SP le «Client Secret».

6. Attributs pour Edulog

La liste des attributs qu'un SP peut attendre de la part de la Fédération est la suivante:

6.1 Prénom

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

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 Catégorie d'âge

Attribute name	EdulogPersonAgeCategory
Description	Catégorie d'âge de la personne
Applicable aux	 
OID (informational)	1.3.6.1.4.1.38688.1.1.1.8
Exemples	6 18
Valeurs permises	• 0 (jusqu'à 6 ans) • 6 (de 6 à 8 ans) • 8 (de 8 à 12 ans) • 12 (de 12 à 14 ans) • 14 (de 14 à 16 ans) • 16 (de 16 à 18 ans) • 18 (18 ans et plus) 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 enseignantes et enseignants (adultes). Il permet de contrôler l'âge et d'en déduire une classe d'âge. Certains SP doivent respecter des restrictions légales concernant l'accès des mineurs à leurs services.

Si une valeur manque dans ce champ pour une personne mineure (détectée par l'attribut EdulogPersonRole), la personne est traitée par défaut comme mineure dans le rang d'âge le plus bas, c'est-à-dire < 6 ans.

Si l'âge d'un ou d'une enseignante (adulte) ne peut pas être déterminé par EdulogPerson-BirthDate, l'attribut EdulogPersonRole ou title est pris en compte. La valeur transmise est alors 18. Si aucun de ces trois attributs n'a une valeur correspondant à un adulte, la valeur transmise est 0 (un mineur au rang d'âge le plus bas).

6.4 Langue

Attribute name	preferredLanguage
Description	Langue de communication primaire 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

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.

6.6 Courriel

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, le courriel est unique. Il s'agit ici de l'adresse courriel professionnelle/scolaire.

6.7 Établissement

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.

6.8 Niveau d'enseignement

Attribute name	EdulogPersonLevel
Description	Niveau d'enseignement 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.

6.9 Cycle

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* = la situation de la personne n'est pas connue.

6.10 Canton

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.

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

6.11 Fonction

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

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 Année de naissance

Attribute name	EdulogPersonYearOfBirth
Description	Année de naissance
Applicable aux	
OID (informational)	1.3.6.1.4.1.38688.1.1.1.7
Exemples	2009 1970 *empty*
Valeurs permises	Commencent dès 1900
Type de données SQL	VARCHAR(4)
Syntaxe LDAP	Numeric String{4}
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 d'en déduire une classe d'âge. Certains SP doivent respecter des restrictions légales concernant l'accès des mineurs à leurs services.
La Fédération déterminera cet attribut en fonction de la valeur de l'attribut *EdulogPerson-BirthDate* fournie par l'IdP. Si une valeur manque dans ce champ, la Fédération vérifie la valeur de l'attribut *EdulogPersonRole* pour déterminer s'il s'agit d'un adulte ou d'un mineur. S'il s'agit d'un adulte, l'année correspondante sera transmise en fonction de l'âge 18 ans. Pour un mineur, l'année correspondant à l'âge de 5 ans.
Syntaxe: Basé sur «Date and Time on the Internet: Timestamps (RFC3339)». Utilisation du format «date-fullyear» du paragraphe 5.6: date-fullyear = 4DIGIT