Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

Vérification de l'identité, qualité des attributs et « Levels of Assurance »

16.9.2025 – Version 1

Dans le cadre d'Edulog, les fournisseurs d'identité (IdP) garantissent que chaque identité qu'ils mettent à la disposition du réseau est attribuée de manière univoque à une personne physique (unicité et exclusivité). Ils garantissent l'exhaustivité, la justesse, la sauvegarde et la mise à jour des attributs associés aux identités qu'ils transmettent au bureau Edulog. En outre, ils assurent la correspondance correcte entre ces attributs et les TechID que les fournisseurs de services reçoivent du secrétariat Edulog, conformément aux exigences légales et réglementaires en vigueur qui s'appliquent aux processus de création, de mutation et de suppression.

Edulog offre aux fournisseurs de services la possibilité de définir les exigences qu'ils posent à la vérification des identités et de leurs attributs par l'IdP. Une distinction est faite entre trois niveaux de sécurité ou de fiabilité (« Levels of Assurance »). Le niveau 3 correspond aux exigences les plus élevées en matière de sécurité et de fiabilité, le niveau 1 aux exigences les plus faibles :

Niveau	Contrôle d'identité	Contrôle d'attributs	Contrôle d'authentification
	Toutes les mesures nécessaires pour immédiatement identifier et enregistrer une identité ; y compris la capacité à relier une identité avec une personne réelle et confirmer que celle-ci est bien active dans le système éducatif.	*Mécanisme pour saisir complètement et correctement tous les attributs déclarés et obligatoires d'une identité et entreprendre à temps les corrections dans la perspective de modifications, y compris la sortie de la personne du système éducatif.*	*Modalités d'exécution de l'authentification y compris de la protection des preuves de légitimation durant la transmission et de la manière dont une personne a un contrôle de fait sur son identité.*
3	Le contrôle d'identité est exécuté par un service indépendant. La constatation de l'identité requiert la présentation d'un ou de plusieurs documents officiels, par exemple le passeport. Une présence physique est nécessaire pour le contrôle d'identité, par exemple au contrôle des habitants.	Tous les attributs mentionnés à l'art. 12 du Règlement d'organisation sont complètement libérés pour les identités. Les attributs sont contrôlés au moins une fois par an et les mutations ou les erreurs sont mises à jour ou corrigées rapidement, c.- à-d. dans les 7 jours. Les adaptations des attributs sont mises en œuvre ou contrôlées par une autorité.	En sus d'une authentification à un seul facteur, une authentification à plusieurs facteurs est également offerte, par exemple via un authentificateur ou un jeton SMS. Une directive de sécurité garantit la qualité des facteurs d'authentification, par exemple via des mots de passe sûrs. Des procédures automatiques et proactives surveillent les activités d'annonce suspectes, par exemple via SIEM.
2	Le contrôle d'identité peut être exécuté sur place, sans être obligatoirement entrepris par un service indépendant, par exemple par l'établissement éducatif.	La majorité des attributs au sens de l'art. 12 du Règlement d'organisation sont libérés pour toutes les identités. En particulier, le prénom, le nom, l'adresse courriel, le rôle, l'institution et le degré de scolarité doivent être impérativement libérés. Les attributs sont contrôlés au moins une fois par an et les mutations et autres erreurs sont actualisées, respectivement corrigées à temps, c.-à-d. dans les 30 jours. Les adaptations de certains attributs, par exemple la fonction, peuvent être effectuées par la personne concernée sous la surveillance d'un service indépendant.	Un seul facteur est utilisé pour l'authentification, par exemple un nom d'utilisateur / un mot de passe. L'utilisation de mots de passe sûrs est recommandée ou encouragée proactivement, par exemple la mesure de la force des mots de passe. Des mesures existent pour garantir la traçabilité de l'activité d'annonce.
1	Il n'y a pas de contrôle d'identité officiel, par exemple par l'auto-enregistrement. Il n'y a pas de liaison fiable de l'identité avec une personne physique unique, (par exemple une confirmation par une adresse courriel).	Les attributs au sens de l'art. 12 du Règlement d'organisation ne sont libérés que partiellement pour toutes les identités. Les attributs ne sont soumis à aucune validation et peuvent être élaborés en tout ou en partie par l'utilisateur lui-même, par exemple via un profil d'utilisateur. Les modifications sont entreprises sans la garantie d'un délai.	Un seul facteur est utilisé pour l'authentification, par exemple un nom d'utilisateur / un mot de passe. L'utilisateur peut choisir ses mots de passe librement et sans restriction.