Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNISCHES

Identitätsprüfung, Qualität der Attribute und «Levels of Assurance»

16.9.2025 – Version 1

Die Identitätsprovider (IdP) stellen im Rahmen von Edulog sicher, dass jede Identität, die sie in der Föderation zur Verfügung stellen, eindeutig einer natürlichen Person zugeordnet ist (Eindeutigkeit und Ausschliesslichkeit). Sie gewährleisten die Vollständigkeit, Korrektheit, Aufbewahrung und Aktualisierung der mit den Identitäten verbundenen Attribute, die sie an Edulog übermitteln. Darüber hinaus gewährleisten sie die korrekte Zuordnung dieser Attribute zu den TechIDs, die die Dienstleistungsanbieter von der Geschäftsstelle erhalten, in Übereinstimmung mit den geltenden gesetzlichen und regulatorischen Anforderungen, die für die Erstellungs-, Mutations- und Löschungsprozesse relevant sind.

Edulog bietet den Service Providern die Möglichkeit festzulegen, welche Anforderungen sie an die Überprüfung der Identitäten und deren Attribute durch den IdP stellen. Dabei wird zwischen drei Sicherheitsstufen bzw. Zuverlässigkeitsgraden («Levels of Assurance») unterschieden. Level 3 entspricht den höchsten Anforderungen an Sicherheit und Vertrauenswürdigkeit, Level 1 den niedrigsten:

Stufe	Identitätsprüfung Alle Massnahmen, die erforderlich sind, um eine Identität sofort zu identifizieren und zu registrieren, einschliesslich der Fähigkeit, eine Identität mit einer realen Person zu verknüpfen und zu bestätigen, dass diese Person tatsächlich im Bildungssystem tätig ist.	Attributsprüfung Mechanismus, um alle deklarierten und obligatorischen Attribute einer Identität vollständig und korrekt zu erfassen und rechtzeitig Korrekturen im Hinblick auf Veränderungen, inklusive Austritts der Person aus dem Bildungssystem, vorzunehmen.	Authentifizierungsprüfung Art und Weise, wie die Authentifizierung durchgeführt wird, einschliesslich des Schutzes von Berechtigungsnachweisen während der Übertragung und inwieweit eine Person die tatsächliche Kontrolle über ihre Identität hat.
3	Die Identitätsprüfung wird von einer unabhängigen Stelle durchgeführt. Zur Feststellung der Identität müssen ein offizielles Dokument oder mehrere solche vorgelegt werden, z.B. Reisepass. Für die Durchführung einer Identitätsprüfung ist eine physische Präsenz erforderlich, z.B. bei der Einwohnerkontrolle.	Alle in Art. 12 des *Organisationsreglements* erwähnten *Attribute* werden vollständig für alle Identitäten freigegeben. Die *Attribute* werden mindestens einmal jährlich geprüft und Mutationen oder Fehler werden zeitnah, d.h. spätestens innert 7 Tagen aktualisiert bzw. korrigiert. Anpassungen der *Attribute* werden von einer Behörde vorgenommen oder überprüft.	Neben Ein-Faktor- wird auch Multifaktor-Authentifizierung angeboten, z.B. durch Verwendung eines Authentifikators oder SMS-Tokens. Eine Sicherheitsrichtlinie gewährleistet die Qualität der Authentifizierungsfaktoren, z.B. durch die Verwendung sicherer Passwörter. Automatisierte und proaktive Prozesse überwachen verdächtige Anmeldeaktivitäten, z.B. via SIEM.
2	Die Identitätsprüfung darf vor Ort durchgeführt werden, ohne dass diese zwingend von einer unabhängigen Stelle vorgenommen wird, z.B. an der Bildungseinrichtung.	Die *Attribute* gemäss Art. 12 des *Organisationsreglements* sind mehrheitlich für alle Identitäten freigegeben. Darunter sind zwingend Vorname, Nachname, E-Mail-Adresse, Rolle, Institution und Bildungsstufe freizugeben. Die *Attribute* werden mindestens einmal jährlich geprüft und Mutationen oder Fehler werden zeitnah, d.h. spätestens innert 30 Tagen aktualisiert bzw. korrigiert. Anpassungen bei gewissen Attributen, z.B. Funktion, können von der *betroffenen Person* unter Aufsicht einer unabhängigen Stelle geändert werden.	Nur ein Faktor wird für die Authentifizierung verwendet, z.B. Benutzername / Passwort. Die Verwendung von sicheren Passwörtern wird proaktiv empfohlen oder gefördert, z.B. durch Messung der Passwortstärke. Es gibt Massnahmen zur Gewährleistung der Nachvollziehbarkeit der Anmeldeaktivität.
1	Es sind keine behördlichen Kontrollen der Identitätsprüfung vorhanden, z.B. Selbstregistrierung. Es besteht keine zuverlässige Bindung der Identität mit einer eindeutigen physischen Person (z.B. Bestätigung durch E-Mail-Adresse).	Die *Attribute* gemäss Art. 12 des *Organisationsreglements* sind nur teilweise für alle Identitäten freigegeben. Die Attribute unterliegen keiner Validierung und können ganz oder teilweise vom Benutzer selbst bereitgestellt werden, z.B. durch Erstellung eines Benutzerprofils. Änderungen werden ohne zeitliche Garantie vorgenommen.	Nur ein Faktor wird für die Authentifizierung verwendet, z.B. Benutzername / Passwort. Der Benutzer darf seine Passwörter ohne Einschränkung frei wählen.