Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kdo Cy / CEA
CoE Software Engineering

Richtlinie zur Anonymisierung von Usern

Version 1.0.0-2-g24d61c2, 16.11.2026

Tabelle 1. Referenzen

Erkennungszeichen	Titel
EMBAG	https://www.fedlex.admin.ch/eli/cc/2023/682/de
BK «OSS Hilfsmittel»	https://www.bk.admin.ch/de/oss-hilfsmittel

Inhaltsverzeichnis

1. Zweck **3**
2. Policy **3**
3. Implementation **4**

1. Zweck

Diese Richtlinie regelt die Anonymisierung von Usern anhand verschiedener Kennzeichentypen. Ziel ist, echte Identitäten möglichst vollständig zu verschleiern und so den Schutz der Privatsphäre zu erhöhen.

2. Policy

Die Richtlinie basiert auf folgenden wesentlichen Aspekten:

- Jeder User besitzt einen Klar-Identifier, z. B. eine U-Nummer oder eine AHV-Nummer.
- Aus diesem Klar-Identifier wird ein anonymisierter Bezeichner erzeugt. Darin sind keine Rückschlüsse auf die echte Identität möglich.
- Die Anonymisierung berücksichtigt unterschiedliche Kennzeichentypen (IdentifierType); jeder Kennzeichentyp ist durch seine eigene Struktur und seinen Wertebereich gekennzeichnet.

Folgende Kennzeichentypen sind festgelegt:

1. LDAP U-Nummer (interne zivile Mitarbeitende)
    - Formatbeispiel: u61234567
    - Wertebereich: 60'000'000 bis 90'000'000
    - Inaktivitätsablauf: 180 Tage
    - GitLab-Gültigkeitsfaktor: 1.5
2. VBS-Kennung (im internen LDAP, z. B. vbs0000001)
    - Formatbeispiel: vbs1234567
    - Wertebereich: 0 bis 3'000'000
    - Inaktivitätsablauf: 60 Tage
    - GitLab-Gültigkeitsfaktor: 0.2
3. Schweizer Sozialversicherungsnummer (AHV)
    - Formatbeispiel: 756.XXXX.YYYY.ZC
    - Wertebereich: 0 bis 1'000'000'000
    - Inaktivitätsablauf: 60 Tage
    - GitLab-Gültigkeitsfaktor: 0.2
4. LDAP UL-Nummer (Armeeangehörige)
    - Formatbeispiel: ul2345678
    - Wertebereich: 1'400'000 bis 10'000'000
    - Inaktivitätsablauf: 60 Tage
    - GitLab-Gültigkeitsfaktor: 0.2

Zur Erzeugung des Anonymisierungskennzeichens werden die folgenden Konstanten

verwendet:

- Domain: swiss-armed-forces-open-source.ch
- ANON_IDENTIFIER_TYPE_ID_LENGTH = 3
- ANON_IDENTIFIER_ID_LENGTH = 9
- ANON_IDENTIFIER_SEPARATOR = "-"
- INITIAL_PASSWORD_LENGTH = 20
- SALT-Identifikationslänge = 3
- PEPPER-Identifikationslänge = 3

Die Anonymisierung erfolgt zusätzlich mithilfe von sogenannten Salts (nicht öffentlich) und Peppers (vertraulich). Dabei wird aus einer Sammlung zufällig ein Salt und ein Pepper gewählt, um bei Bedarf mehrmals verschiedene Anonymisierungen für ein und dieselbe Person zu ermöglichen.

3. Implementation

Die Umsetzung der Richtlinie folgt diesem Prozess:

1. Erkennung des Kennzeichentyps:

   Zunächst wird das eingegebene Klar-Kennzeichen geprüft, um festzustellen, zu welchem Kennzeichentyp es gehört und ob es sich im erlaubten Wertebereich befindet.

2. Ziehung der Seasonings (Salts und Peppers):

   Aus bestehenden Sammlungen wird ein Salt und ein Pepper zufällig ausgewählt, damit jeweils neue Variation(en) eines anonymen Kennzeichens möglich sind.

3. Erzeugung des Anonymisierungskennzeichens:

   - Aus einer Wortliste werden zwei Adjektive und ein Nomen gewählt.
   - Diese drei Teile (z. B. «welcoming-khaki-orchid») werden ergänzt um:
     - die ID des gewählten Salts
     - die ID des gewählten Peppers
     - einen verkürzten Hash-Wert für den Kennzeichentyp
     - einen verkürzten Hash-Wert für den Klar-Identifier
   - Alle Elemente sind durch das Trennzeichen "-" miteinander verbunden, zum Beispiel: `ad1-ad2-noun-sID-pID-tHash-iHash`

4. Generierung und Zuordnung der Anonymisierungsattribute:

   - Der User erhält eine anonyme E-Mail-Adresse in folgender Form: `anonymisiertesKennzeichen@swiss-armed-forces-open-source.ch`
   - Vorname und Nachname werden aus den beiden Adjektiven und dem Nomen abgeleitet.
   - Zusätzlich wird ein zufälliges Initialpasswort mit einer Länge von 20 Zeichen

erzeugt.

5. Ausgabe der anonymisierten Werte:
    - identifier: das komplette Anonymisierungskennzeichen
    - email: daraus generierte E-Mail-Adresse
    - first_name und last_name: zwei Adjektive bzw. ein Nomen
    - initial_password: zufällige 20-stellige Zeichenkette aus Buchstaben und Ziffern

Durch diese Vorgehensweise wird die Privatsphäre der User unter Einhaltung oben genannter Parameter und Konstanten gewahrt.