Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kdo Cy / CEA
CoE Software Engineering

Richtlinie zur Deanonymisierung 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 **3**

1. Zweck

Diese Richtlinie ermöglicht das Rückführen zuvor anonymisierter User-Kennungen auf die ursprünglichen Klar-Identifikatoren. Damit wird die Möglichkeit geschaffen, bestimmte administrative oder audit-bezogene Anforderungen zu erfüllen, indem anonymisierte Identifikatoren wieder auf echte User abgebildet werden können.

2. Policy

Die Richtlinie sieht vor, dass zuvor erstellte, anonymisierte User-Kennungen wieder deanonymisiert werden können. Dabei gilt Folgendes:

- Um die Anonymisierung aufzuheben, müssen alle relevanten «Salts» und «Peppers» verfügbar sein. Standardmässig werden sie aus Dateien geladen, die in den Konstanten DEFAULT_SALTS_FILE (salts) und DEFAULT_PEPPERS_FILE (peppers) definiert sind.
- Für jedes anonymisierte Identifikator-Format werden Minimal- und Maximalwerte als Suchbereich verwendet. Die aktuellen Werte lauten:

  Typ 1 (LDAP U-Nummer)

  min_value = 60'000'000, max_value = 90'000'000, inactivity_expiration = 180 Tage, gitlab_validity_factor = 1.5

  Typ 2 (VBS-Identifikator)

  min_value = 0, max_value = 3'000'000, inactivity_expiration = 60 Tage, gitlab_validity_factor = 0.2

  Typ 3 (AHV-Nummer)

  min_value = 0, max_value = 1'000'000'000, inactivity_expiration = 60 Tage, gitlab_validity_factor = 0.2

  Typ 4 (LDAP UL-Nummer)

  min_value = 1'400'000, max_value = 10'000'000, inactivity_expiration = 60 Tage, gitlab_validity_factor = 0.2

- Die Grösse der Einzelschritte bei der Suche pro Prozess ist durch IMAP_CHUNK_SIZE = 1000 festgelegt.

3. Implementation

Für die Deanonymisierung führt die Funktion cmd_deanon_identifiers die folgenden Schritte durch:

1. Laden der Seasonings: Es werden die Salt- und Pepper-Werte aus den definierten Dateien geladen.
2. Aufteilung nach Identifikator-Typ: Alle anonymisierten Kennungen werden zunächst analysiert, um den zugehörigen IdentifierType zuzuordnen.
3. Durchsuchen des Wertebereichs: Für jeden IdentifierType wird eine schrittweise Suche innerhalb der min_value- und max_value-Grenzen durchgeführt, um eine Übereinstimmung des berechneten Hashes mit dem anonymisierten Hashwert zu

finden.

4. Zuordnung von Treffern: Falls eine Übereinstimmung vorliegt, wird die Klar-Identifikation (z. B. eine U-, VBS-, AHV- oder UL-Nummer) dem anonymisierten Kennzeichen zugeordnet.