Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kdo Cy / CEA
CoE Software Engineering

Richtlinie zur Deanonymisierung aller GitLab-User

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 regelt die Deanonymisierung sämtlicher anonymen User der GitLab-Gruppe in einem einzigen Durchgang. Sie ergänzt die «Richtlinie zur Deanonymisierung von Usern», die einzelne Kennungen auflöst, für administrative oder audit-bezogene Zwecke, bei denen alle User betroffen sind.

2. Policy

- Grundlage sind die SAML-Identitäten der obersten GitLab-Gruppe (swiss-armed-forces, GITLAB_GROUP_ID = 90701827). Jede SAML-Identität enthält die anonyme Kennung als lokalen Teil der E-Mail-Adresse: `<anonyme Kennung>@swiss-armed-forces-open-source.ch`.
- Ausgenommen sind:
  - Bots: Kennungen nach dem Muster `group_<Nummer>_bot_<Hex>` oder `project_<Nummer>_bot_<Hex>`
  - Administratorkonten: die Kennung `admin`, auch mit angehängten Ziffern (z. B. `admin1`)
- Die Deanonymisierung selbst folgt der «Richtlinie zur Deanonymisierung von Usern»: dieselben Salts und Peppers, dieselben Wertebereiche und dieselbe Suche.
- Kennungen, die sich nicht auflösen lassen (unbekanntes Format, unbekannter Identifier-Typ oder Pepper), werden mit einer Warnung übersprungen.
- Das Ergebnis ist eine Zuordnung im JSON-Format: jede anonyme Kennung mit der Liste der gefundenen Klar-Identifikatoren (z. B. einer U-Nummer).
- Das Ergebnis enthält die echten Identifikatoren der User. Es ist vertraulich zu behandeln, wird nicht im Repository abgelegt und nach Gebrauch gelöscht.

3. Implementation

1. Die SAML-Identitäten der obersten GitLab-Gruppe werden über die GitLab-API gelesen; dafür ist ein GitLab-Access-Token erforderlich.
2. Bots und Administratorkonten werden entfernt, aus den übrigen Identitäten wird die anonyme Kennung entnommen.
3. Für diese Kennungen wird die Deanonymisierung gemäss «Richtlinie zur Deanonymisierung von Usern» durchgeführt.
4. Die Zuordnung wird als JSON in die mit `-o` angegebene Datei geschrieben, ohne `-o` auf die Standardausgabe.