Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kdo Cy / CEA
**CoE Software Engineering**

# Richtlinie zur Erzeugung von Salts und Peppers

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 hat zum Ziel, eindeutige und ausreichend grosse Kollektionen von Seasonings zu erstellen, um Kollisionen bei der späteren Verwendung in Hash-Funktionen zu vermeiden. Dafür werden sowohl Salts als auch Peppers in vordefinierter Anzahl generiert und innerhalb festgelegter Parameter auf Kollisionen überprüft.

## 2. Policy

Die Richtlinie sieht vor, dass für Salt-Seasonings und Pepper-Seasonings jeweils eine definierte Anzahl Einträge bereitgestellt wird. Dieser Wert beträgt für Salts 2'048 und für Peppers 2'048. Alle Salt-Seasonings müssen die Bedingung erfüllen, dass sie unter den reservierten Identifier-Typen (Indexbereich 0 bis 99) keine Hash-Kollisionen erzeugen. Peppers unterliegen keiner Kollisionsprüfung, da nur das Salt in den Hash des Identifier-Typs eingeht.

Die wesentlichen Konstanten dieser Richtlinie lauten:

- SALTS_COUNT = 2'048
- PEPPERS_COUNT = 2'048
- RESERVED_IDENTIFIER_TYPE_IDS = Werte von 0 bis 99

## 3. Implementation

Um die Richtlinie umzusetzen, wird ein Prozess durchlaufen, der Folgendes sicherstellt:

1. Salts werden so lange erzeugt, bis 2'048 gültige Salt-Seasonings vorliegen. Jedes Salt wird verworfen, sobald zwei reservierte Identifier-Typen denselben Hash ergeben. Nur Salt-Seasonings ohne Kollisionen werden akzeptiert.
2. Peppers werden so lange erzeugt, bis 2'048 Pepper-Seasonings verfügbar sind. Eine Kollisionsprüfung entfällt (siehe oben).
3. Die schliesslich gesammelten Salt-Seasonings und Pepper-Seasonings werden in separaten Dateien abgespeichert, um später für Benutzeridentifikations- und Hash-Zwecke eingesetzt zu werden.