

STACKIT GmbH & Co. KG
Stiftsbergstraße 1 | 74172 Neckarsulm

Service Certificate STACKIT Secrets Manager

Service name

STACKIT Secrets Manager

High level service description

STACKIT Secrets Manager ("Secrets Manager") is a managed service that provides a secure key-value store for sensitive data (such as passwords, configuration files and text). It enables the protection and management of secrets. The Secrets Manager provides an API that enables easy integration into applications and workflows. This allows the separation of source code and secrets, and compliance requirements can be implemented.

Key Features

- Storage of secrets according to security requirements (e.g., separation of source code and secrets)
- The customer can order a Secrets Manager fast and simply using the self-service user interface in the STACKIT Portal
- Secrets can be managed via a user-friendly configuration interface and API
- Traceability of changes through versioning of individual secrets
- High availability guarantees the safe operation of the Secrets Manager
- Pre-configured auto-update functions keep components up-to-date

Service Plans

The Secrets Manager automatically scales in the number of secrets, secret versions and users.

The following limitations apply:

- the number of API accesses per Secrets Manager is limited to 10,000 accesses per hour
- up to 100 users can be created per Secrets Manager

up to 1 MB of text can be stored in the form of key-value pairs for each secret version

Metric

Billing takes place by the hour according to the number of secret versions.

SLA specifics

- Secrets Manager is considered available as long as the API and configuration interface are accessible at the service delivery point.

Backup

- There is no customer-specific backup. The Secrets Manager automatically saves a preconfigured number of secret versions (unlimited by default). If a version limit is set and exceeded the oldest versions will be deleted.

Additional terms

The customer is responsible for the configuration of Secrets Manager (in particular the management of accounts and version limit).

Annex: Exportability (Online Register)

Data Type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data (Database Content)	Data stored by the customer in the database (if available) or within the product/service	Yes	JSON	Data export is possible via the Hashicorp compatible API
User Accounts & Permissions	User for STACKIT Secrets Manager	Yes	JSON	The password can not be exported
	STACKIT Identity & Access Management (IAM) User	Yes	JSON	Exportable via STACKIT IAM API
System Metrics (Instances / Resources in Use)	Performance data of the instance / resource in use (e.g., CPU usage, memory usage)	No. Company confidential STACKIT.	-	
	Sizes and Capacities <i>Capacities of the available resources / instances</i>	Yes	JSON	Amount of Secrets and Versions
System properties (Instances / Resources in use)	Versions and information necessary to check compatibility	No. Company confidential STACKIT.	-	
Product / service-related	Configuration data and source code	No. Company confidential STACKIT.		

data (product properties)	Log Data (non personalized and personalized)	No. Company confidential STACKIT.		
	Log Data (non personalized and personalized) Login/Logout of User, User activities	Yes	JSON	Events can be exported via the STACKIT Auditlog API

Version and start of validity

Version 1.4, valid from 12.09.2025

STACKIT GmbH & Co. KG
Stiftsbergstraße 1
D-74172 Neckarsulm

Tel: +49 (0) 7132-30474747
info@stackit.de
www.stackit.de

Kommanditgesellschaft mit Sitz Neckarsulm
Amtsgericht Stuttgart HRA 741347
USt-IdNr. DE368560082

Commerzbank AG
DE55 6004 0071 0521 9928 00
SWIFT/BIC: COBADEFFXXX

Komplementärin: STACKIT Beteiligungs-GmbH | Sitz: Neckarsulm | Registergericht: Stuttgart, HRB 795936
Geschäftsführer: Christian Müller, Robin Hermann