STACKIT GmbH & Co. KG
Stiftsbergstraße 1 | 74172 Neckarsulm

Leistungsschein – STACKIT Key Management Service

Servicename
STACKIT Key Management Service

Kurzbeschreibung
STACKIT Key Management Service („**KMS**“) ist ein von STACKIT gemanagter Service, der die Erstellung, Verwaltung und Verwendung von kryptografischen Schlüsseln („**Schlüssel**“) für den Kunden vereinfacht.
Er ermöglicht es dem Kunden, kryptografische Operationen sicher und effizient durchzuführen. Die KMS-API macht es einfach, die Schlüsselverwaltung in Anwendungen und Arbeitsabläufe des Kunden zu integrieren.

Wesentliche Merkmale
- Der Kunde kann KMS Schlüssel für sich generieren lassen oder eigene Schlüssel (die den definierten Standards entsprechen) mitbringen, indem diese verschlüsselt zu KMS hochgeladen werden
- Kryptographische Schlüssel können in den folgenden Varianten generiert werden: AES-256, RSA-2048, RSA-3072, RSA-4096
- Das Rotieren von Schlüsseln („Key Rotation“) ist möglich
- Ermöglicht das Verschlüsseln und Entschlüsseln von Daten des Kunden mit im KMS gespeicherten Schlüsseln
- Schlüssel können sowohl über eine benutzerfreundliche Konfigurationsoberfläche als auch via API verwaltet werden
- Hochverfügbarkeit gewährleistet den sicheren Betrieb des KMS

Servicepläne
KMS skaliert automatisch mit der Anzahl der vom Kunden verwendeten Schlüssel und Schlüssel-Versionen.

Es gibt folgende Beschränkung:
- die Anzahl der API-Zugriffe ist je KMS auf 10.000 Zugriffe pro Stunde beschränkt
- die Größe der Entschlüsselungs-/Verschlüsselungsdateien ist auf 64 kB beschränkt

Metrik
Der Kunde hat die Möglichkeit die Anzahl der von ihm verwendeten Schlüssel-Versionen selbst zu verwalten, insbesondere diese zu erstellen bzw. zu löschen. Die Abrechnung erfolgt stundengenau nach der jeweils vorhandenen Anzahl an Schlüssel-Versionen des Kunden je angefangener Stunde.

SLA-Spezifika

- KMS gilt als verfügbar, sofern die API und die Konfigurationsoberfläche am Leistungsübergabepunkt erreichbar sind.

Backup

- Es findet kein kundenindividuelles Backup statt.

Zusätzliche Bedingungen

- Der Kunde ist für die Konfiguration des KMS und seiner Schlüssel verantwortlich.
- Der Kunde wird darauf hingewiesen, dass Schlüssel, die gelöscht wurden, nicht mehr verwendet werden können. Ein gelöschter Schlüssel kann innerhalb von 30 Tagen wiederhergestellt werden. Sind Daten mit gelöschten Schlüsseln verschlüsselt, können diese Daten nicht mehr entschlüsselt werden.

Anhang: Exportierbarkeit (Online Register)

Datentyp	Beschreibung	Exportierbar (Ja/Nein)	Format	Zusätzliche Anmerkungen
Kundendaten (Datenbankinhalte)	Daten, die vom Kunden in der Datenbank (sofern vorhanden) bzw. innerhalb des Produktes/Services gespeichert werden	Ja	JSON	Der Export von Kundendaten ist über die KMS-API im JSON-Format möglich. Dies umfasst Metadaten, die zur Wiederherstellung der Schlüsselarchitektur notwendig sind, um die Datenportabilität zu gewährleisten
Benutzerkonten & Berechtigungen	STACKIT Identity & Access Management (IAM) Benutzer	Ja	JSON	Über die STACKIT IAM API exportierbar
System Metriken (Instanzen / Ressourcen in Nutzung)	Leistungsdaten der Instanz/ genutzten Ressource (z. B. CPU-Auslastung, Speichernutzung)	Nein. Betriebsinternum STACKIT.	-	
	Größen und Kapazitäten Kapazitäten der vorhandenen Ressourcen / Instanzen	Ja	JSON	Anzahl an Schlüsselringen, Schlüsseln und Versionen
Systemeigenschaften (Instanzen / Ressourcen in Nutzung)	Versionen und Informationen, die notwendig sind um Kompatibilität prüfen zu können	Nein. Betriebsinternum STACKIT.	-	

Produkt / Servicebezogene Daten (Produkteigenschaften)	Konfigurationsdaten und Source Code	Nein. Betriebsinternum STACKIT.	-	
	Log Daten (nicht personalisiert und personalisiert)	Nein. Betriebsinternum STACKIT.	-	
	Log Daten (nicht personalisiert und personalisiert) Login/Logout der Nutzer, Nutzeraktivitäten	Ja	JSON	Events können über die STACKIT Audit Log API expotiert werden

Version und Geltungsbeginn
Version 1.1, gültig ab 12.09.2025