schwarz digits

Service certificate

STACKIT Key Management Service

Version and start of validity	
Version 1.1	Valid from 2025/09/12

Service certificate | STACKIT Key Management Service

Service name

STACKIT Key Management Service

High level service description

STACKIT Key Management Service („**KMS**“) is a managed service that simplifies the creation, management, and use of cryptographic keys (“**keys**”).
It allows the customer to perform cryptographic operations securely and efficiently.
The KMS API simplifies to integrate key management into the customer’s applications and workflows.

Key features

- Customers can either have KMS keys generated for their use or bring their own keys (that comply with the defined standards) by uploading them to KMS in encrypted form.
- Generate cryptographic keys of the following variants: AES-256, RSA-2048, RSA-3072, RSA-4096
- “Key Rotation” is possible
- Enables the encryption and decryption of customer data with keys stored in KMS
- Manage keys via an user-friendly configuration interface or via API
- High availability ensures the safe operation of the KMS

Service plans

KMS automatically scales with the number of keys and key versions used by the customer

The following limitation applies:

- the number of API accesses is limited to 10.000 accesses per hour per KMS
- the size of the decryption / encryption files is limited to 64 kB

Metrics

- The customer is able to self-manage the number of key versions in use, including creating and deleting them as needed. Billing per hour, based on the number of available key versions.

SLA specifics

- KMS is considered available insofar the API and configuration interface are accessible at the service delivery point.

Backup

- There is no customer specific backup.

Additional terms

- The customer is responsible for the configuration of KMS and its keys.
- Keys that the customer deletes can no longer be used. A deleted key can be recovered within 30 days. If data is encrypted with deleted keys, it’s not possible to decrypt this data.

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	The export of customer data is possible via the KMS API in JSON format. This includes metadata necessary to restore the key architecture, ensuring data portability.
User accounts & permissions	Information about users and their permissions	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 *Capacities of the available resources / instances*	Yes	JSON	Amount of Keyrings, Keys and Versions
System properties (instances / resources in use)	Versions and information necessary to check compatibility	No. Company confidential STACKIT.	-	-
Product / service-related data (product properties)	Configuration data and source code *Configuration of IT-systems / rudimental IT, settings, customizing, IP's, VLAN, interfaces, software code, scripts*	No. Company confidential STACKIT.	-	-

Log data (non personalized and personalized) *System-status, technical-events, etc*.	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