



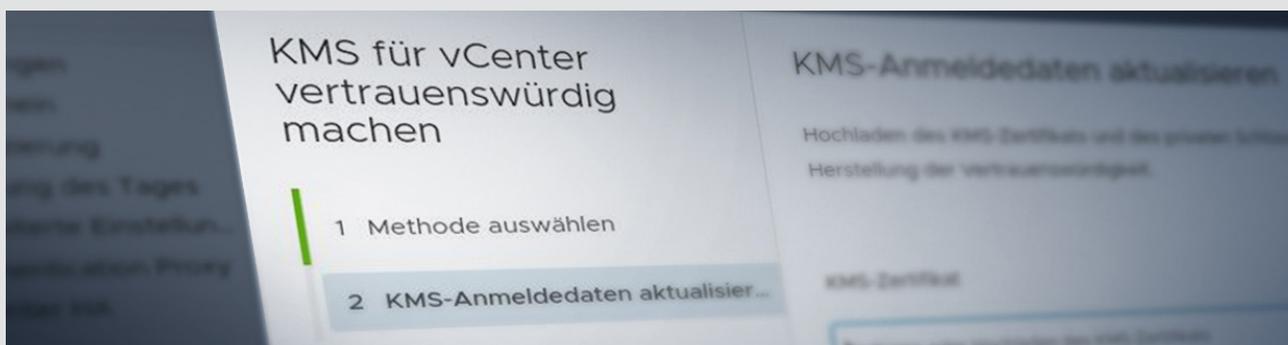
## MTG KMS for VMware Encryption

The MTG Key Management System enables users to encrypt their VMware virtual machines with few clicks, helping to protect their critical and sensitive data quickly and easily. This is realized by innovative VMware Encryption-as-a-Service offerings in cooperation with the infrastructure provider DARZ GmbH.

### Why VMware Encryption with a external KMS?

With a changing and growing threat landscape, operators of virtual machines (VMs) increasingly have to deal with the issue of encrypting their critical data. VMs are portable and can therefore run on any server. Unauthorized internal persons or external attackers who have gained access to the relevant networks are able to access the data of unencrypted VMs without any protection. Data is virtually served "to-go".

An external KMS allows much more flexibility in the setup and introduction of innovative services. Once connected, users can very easily encrypt selected VMs from VMware. MTG's new Key Management System is designed to enable these companies to effectively encrypt their VMware virtual machines quickly and cost-effectively.



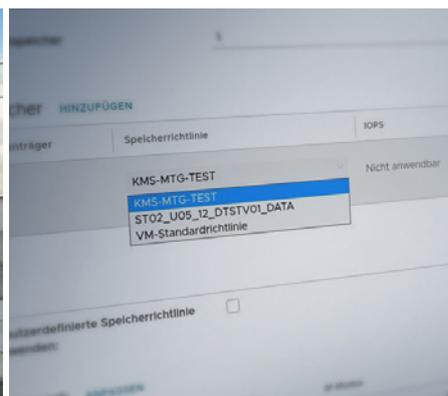
*For hackers unencrypted data on virtual machines are virtually served "to-go".*

# MTG Key Management System for VMware Encryption VMware Encryption-as-a-Service

## New Service by DARZ

In cooperation with DARZ GmbH, a long-term partner and infrastructure provider, a new VMware Encryption-as-a-Service has been created, enabling customers to encrypt their VMware quickly and easily.

- > Via the familiar user interface of the vCloud Director for managing the VMs, the DARZ customers can book and use the offer with just a few clicks.
- > A particularly attractive feature is the possibility of having the VMs, which are operated in one's own data center, reliably encrypted via the DARZ service, completely independent of location.
- > Besides encrypting VMs, VMware also offers the option of protecting so-called vSANs.
- > Further Services: The great advantage of a standard interface like KMIP is its vendor independence. This opens up a lot of opportunities for further IT security services on the basis of the MTG KMS, such as the encryption of KMIP-based databases, tape drives or other storage solutions – for example as NetApp.



### VMware Encryption for data center operators

Data center operators have the choice to connect to the DARZ Services or to run their own KMS: In this case the MTG KMS is installed and configured in a failsafe manner in cooperation with the data center. The KMS is connected to VMware's vCenter via the existing KMIP interface. On this basis, data center operators can create attractive offers for their customers that enable the encryption of VMs from VMware virtually by the push of a button.



*The new DARZ service enables VMware virtual machines to be encrypted reliably and completely independent of their location.*



SecurITy  
Trust Seal  
www.trust.de/itmig  
made  
in  
Germany

MTG AG is a leading specialist for sophisticated encryption technologies "Made in Germany". We simplify and centralize the management of cryptographic keys and identities throughout the complete key management lifecycle.

MTG AG · Dolivostrasse 11 · 64293 Darmstadt · Germany  
Tel +49 6151 8000-0 · [contact@mtg.de](mailto:contact@mtg.de)

# MTG

[mtg.de](http://mtg.de)