T Systems

External Key Management for AWS

How do I control my data independently of a cloud service provider?

Data residency regulations are constantly changing globally, and it is becoming difficult for decision makers to take the required steps in order to comply with the changes. Security and risk management leaders must take urgent action to mitigate security, privacy, and data residency risks.

Data residency across cloud services creates complex choices about balancing business needs against growing risks to provide adequate data security and compliance. This is due to the impacts of access by cloud service providers, government authorities, and staff located around the world.

Discussions about secure cloud usage boil down to the question of the storage and access of encryption keys. Encryption is an essential part of a sophisticated security strategy for the cloud. However, the keys for encryption are stored in a specific key management service on the hyperscaler platform. This impedes the AWS cloud usage in regulated industries or for data-sensitive workloads. Enterprises, thus, tend to run their respective applications in an environment that they can control better. Avoiding discussions with regulatory authorities, but this means they are not able to leverage the advantages of the cloud for these workloads.

Keys reside in the EU and are managed by Telekom – the leading security provider in Germany.

T-Systems , a subsidiary of Deutsche Telekom, is the market leader in security in Germany. Telekom has years of expertise delivering, solutions to customers with a holistic, convergent, and integrated security management across the value chain. This includes people and processes, infrastructure and technology, products and services, and data and information. T-Systems provides encryption keys from Telekom data centers based in Germany, or other EU locations. External Key Management is operated outside of the AWS platform and AWS does not have access to the customer keys. T-Systems acts as a custodian for the keys used on AWS.

Our approach to encryption on AWS

T-Systems provides a highly available, scalable, and secured infrastructure for customers to use AWS. The keys are hosted in a high-availability Telekom data center in hardware security modules (FIPS 140–2 level 3 validated HSM), which are either dedicated for a customer or shared, depending on customer preferences and requirements. Security software (CipherTrust Manager, CTM) from Thales is used as a base. This software fulfills the highest security standards. On the AWS side, Key Management Services (KMS) are connected with these backend systems. Thus, a KMS external key store (XKS) in the customer's AWS account is established. The customer can use the keys mostly in the same way as normal AWS managed KMS keys, i.e., the keys integrate nicely with all the AWS services supporting KMS.

T-Systems provides a self-service interface for customers for key creation, modification, and deletion. T-Systems will be responsible for the management of the key infrastructure, including the setup of a highly available infrastructure.

The EKM service supports regulatory compliance and auditing requirements by logging and monitoring of key operations.

External Key Management: Implementing encryption in the AWS Cloud

01 **Key infrastructure:** Hosted in Deutsche Telekom data centers in Germany and other EU locations. Deutsche Telekom/T-Systems is the leading security provider in Germany.

02 **Encryption keys managed outside the cloud:** Key encryption is handled outside AWS giving customers a vendor-independent control.

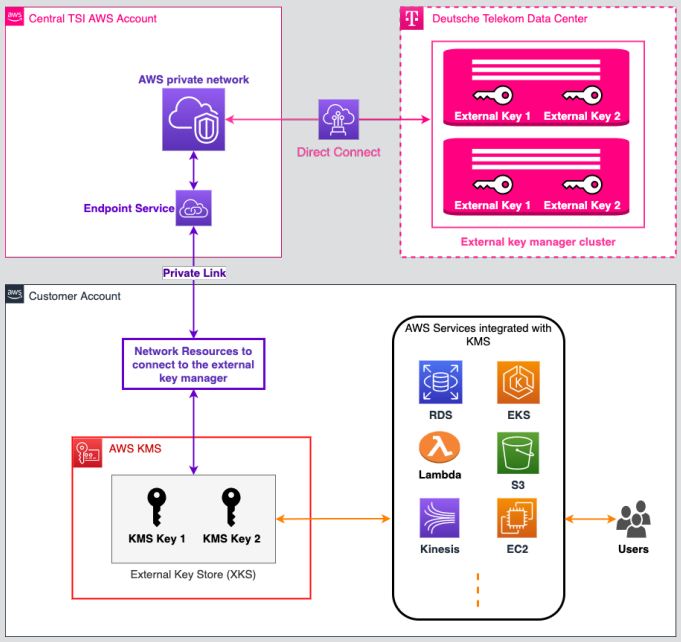
03 **Encryption keys are stored via secure hardware:** Keys are stored in FIPS 140–2 Level 3 validated Hardware Security Module (HSM).

04 **Supports regulatory compliance:** Allows customers to encrypt data and applications handling sensitive data in a safe and confidential way. Also, helps address compliance with government and industry regulations.

05 **Seamless integration with AWS Services:** Integration with a majority of AWS Services being used by AWS Key Management Services.

06 **Key access auditing:** Logging and monitoring of key operations.

07 **Highly available and scalable infrastructure:** Keys are hosted in highly available infrastructure in Telekom data centers. AWS Services are connected to the data centers using redundant IPSec Site-to-Site VPN connections.



Source: Amazon Web Services

Our AWS security experts are here to answer your questions and to do a POC for the solution. Get in touch today and take your next step to a secure and successful future with AWS.

"We take GDPR compliance very seriously at ITONICS, so when we were researching how to comply with the Schrems II ruling, we started looking for ways to encrypt our data with keys managed inside the EU. We were delighted to be invited to Deutsche Telekom's Key Management Service beta program to test the integration with a number of AWS services. The results of these tests were positive, and we are now moving to the implementation phase of the project."

Martin Hignett, CTO ITONICS GmbH

T Systems

Contact

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Tel: 00800 33 090300
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Publisher

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main, Germany