External Key Management for an automotive manufacturer

Case Study

Executive summary

Customers from around the world often tell that digital sovereignty is a top priority as they look to meet new compliance and industry regulation.

A major German automotive manufacturer, particularly was looking for a Key Management Solution that can be deployed independent of cloud service provider as well as is provided and managed by a local trusted vendor, helping them to secure their data at rest on AWS with operational autonomy.

T-Systems successfully brought in their “External Key Management Solution” (EKM). It runs in T-Systems own data centers in EU and uses the AWS KMS external key store capability. This allows the customer to incorporate their own encryption keys that remain solely under their control during the en-/decryption process without the complexity of operating their own external key infrastructure.

Customer challenge

To enhance sovereignty over their data stored in AWS cloud, our customer from the automotive sector was looking for a solution, where the encryption keys used in the data encryption process are managed outside of AWS, ensuring that they have full and independent control.

The external key store feature from AWS KMS has been identified to meet their data sovereignty needs. However, implementing this feature presented additional challenges that required careful consideration and eventually they were looking for a trusted local partner to assist with these complexities:

01 **Complexity of Operating Hardware Security Modules (HSM):**

- Availability and Reliability: Ensuring the HSM’s uptime is critical, as downtime affects access to encrypted data and application availability.
- Continuous Monitoring: Regular monitoring is required to maintain system health and performance.
- Maintenance: Ongoing maintenance is essential to keep the HSM operational and secure.
- Compliance Audits: Periodic audits are necessary to ensure compliance with regulatory requirements.

02 **Secured Connection Complexity:**

- Establishing Secure Connections: Creating and maintaining secure connections between AWS applications and the external key manager outside of the cloud involves complex configurations and robust security measures.

03 **Key Management Complexity:**

- Creating and Managing Keys: Managing the lifecycle of encryption keys, from creation to rotation and destruction, within an external key manager adds significant complexity to the overall system.

Solution

T-Systems supported this customer in implementing the AWS External Key Store (XKS) service while adhering the compliance requirements addressed by their security department by providing its External Key Management Solution (EKM).

T-Systems EKM value proposition focuses on three areas:

- Operating the external key manager, highly available and secure out of a European data centers
- Connecting AWS KMS to the external key manager
- Allowing to manage XKS KMS keys as self service

T Systems

The external key manager used is a software-based Hardware security Module (HSM) called Cypher Trust Manager (CTM) provided by Thales. Telekom's security experts manage this CTM in two clusters across multiple Telekom data centers (availability zones) fulfilling georedundancy and disaster recovery requirements.

The CTM serves as the primary tool for generating and storing external keys. Within each availability zone, every cluster node is synchronized, ensuring that they all possess identical copies of the keys. Additionally, these nodes are supported by a cluster of Luna Hardware Security Modules (HSMs) provided by Thales, strategically deployed across two Deutsche Telekom datacenters in Europe, ensuring robust high availability. The Luna HSMs are used in this setup only as root trust for the CTM clusters and not used for managing encrypting keys.

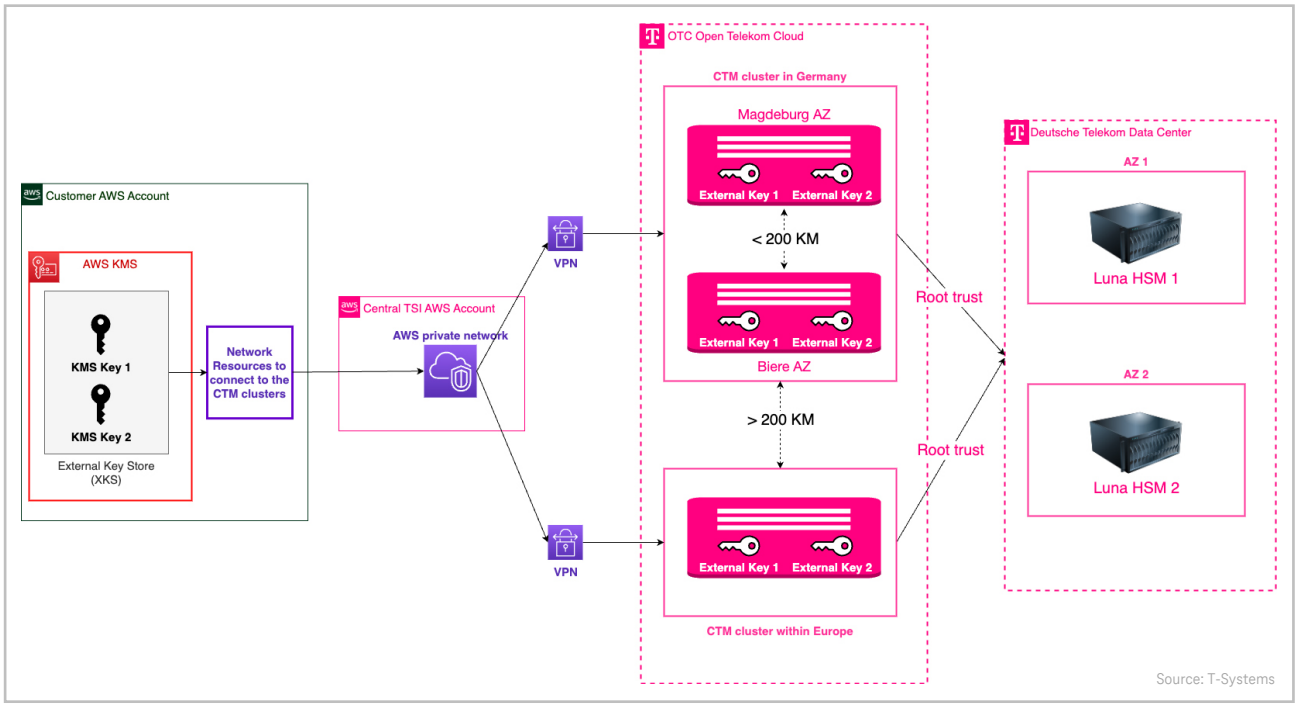
EKM includes a private network in a T-Systems (TSI) AWS account that is connected to the CTM clusters via two AWS IP-Sec VPN connections each terminating from the AWS side in different region for high availability.

From this central network, we distribute the connection to our customers AWS account and region where they require EKM service using AWS private link.

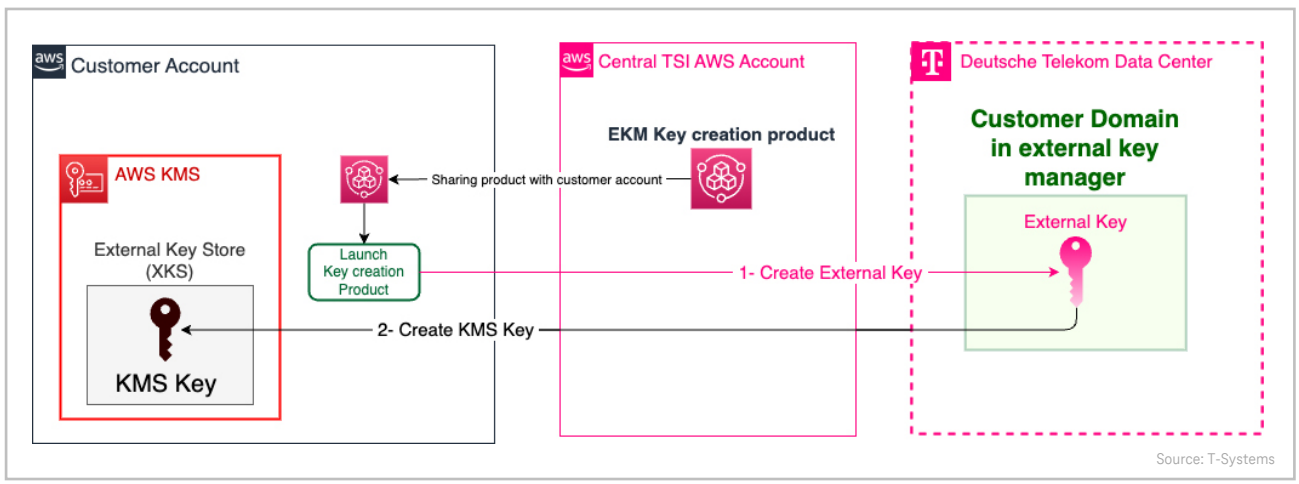
Using AWS IPsec VPN and AWS PrivateLink offers significant value in terms of security, privacy, and reliability.

To enable this connectivity, some network and other AWS resources needed to be created in the customer's AWS account. This includes AWS VPC, AWS subnets, AWS Endpoint services, AWS Network Load Balancer, and IAM role to manage external key stores and the XKS KMS keys.

The following diagram shows the EKM Product:



Additionally, EKM enabled seamless and secure XKS KMS key creation for the customer through a fully automated self-service product, accessible within their account. This product leverages the AWS Service Catalog service, as illustrated in the diagram below:



The Service Catalog product is administered within a portfolio in the central AWS T-Systems EKM account. This portfolio is shared with EKM's customer AWS account. Through the access functionality within the AWS Service Catalog service portfolio, the customer can designate the IAM User, Role, or group authorized to launch the product and create XKS KMS keys that are backed by external keys automatically.

The created keys use AES-256 encryption. The product keeps a detailed record of each interaction with the external key manager. This enables the tracking of each external key usage. Automation for external keys rotation is in progress.

AWS Service Catalog offers seamless integration with other AWS services like CloudFormation, API Gateway, Lambda, and more. This integration is particularly beneficial for key creation in application deployment, ensuring efficient and secure management of resources.

Results and benefits

The solution now allows our customer from the automotive sector to fulfil their data sovereignty requirements by encrypting vehicle-related data using the external key store feature from AWS KMS, ensuring that AWS has no access or control over these keys.

Contact
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: info@t-systems.com
Internet: www.t-systems.com

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

T Systems