

Security - Customer unable to modify existing key on Azure SQL Server and key validation failures

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:23 AM PDT

Contents

- [Issue](#)
- [Investigation/Analysis](#)
- [Mitigation](#)
- [RCA Template](#)
- [Public Doc Reference \(optional\)](#)
- [Internal Reference \(optional\)](#)
- [Root Cause Classification](#)

Issue

Customers unable to update/modify existing Keys in Azure SQL Server

Investigation/Analysis

If the customer is using a third-party service provided by Thales (Cipher) this scenario is impacting during key modification or update.

Mitigation

Customers need to wait for 24 hours after importing the Key into AKV before they can use it for Azure SQL DB TDE.

RCA Template

Due to a key format difference between the Thales CipherTrust Manager and Azure SQL Server, the key retrieved by the Azure SQL Server configured with the key vault was not compatible with the standard Windows crypto APIs.


This caused the TDE key validation workflows on the SQL side to error out preventing the addition of the key to the SQL server.

After 24 hours a key normalization process in the Azure Key Vault service changed the formatting of the key into the expected format, causing the subsequent key operations to succeed.

Thales (Third-party service provider) has logged an issue (KY-42033) in their public documentation with a fix planned for CipherTrust Manager v2.8.0.

Further details can be found here: https://thalesdocs.com/ctp/cm/2.6/release_notes/index.html 

Public Doc Reference (optional)

Third-Party public [documentation](#)  from Thales has mentioned clearly the issue and reported it will be having a fix for this in 2.8 release.

KY-42033 - Unable to use the key version created through CCKM for Azure SQL EKM. This issue will be resolved in CipherTrust Manager v2.8.0.

Internal Reference (optional)

Master ICM to link support cases - <https://portal.microsofticm.com/imp/v3/incidents/details/286543544/home> 

Root Cause Classification

Security/TDE/Issue/Thirdparty

How good have you found this content?



-