FAQ: Vormetric Key Management – Key Agent for Microsoft SQL Server Transparent Data Encryption

Contents

Document Version: ................................................................................................................................... 2
Overview ................................................................................................................................................... 2
Acronyms .................................................................................................................................................. 2
Microsoft SQL Server 2008 & SQL Server 2012 TDE ................................................................................. 3
Public Key Cryptography Standard (PKCS) ................................................................................................ 3
Vormetric Key Manager and Microsoft SQL Server TDE ........................................................................... 4
Microsoft SQL Server TDE Use Cases ........................................................................................................ 5
Vormetric Key Agent – Audit Logging ....................................................................................................... 5
Vormetric Data Security Manager, Key Agent and Microsoft SQL Server TDE keys ................................. 5
Licensing .................................................................................................................................................... 6
Vormetric Key Agent - Supported platforms ............................................................................................ 7
References ................................................................................................................................................ 7
Overview

Vormetric has introducing a new product to the Vormetric Data Security to provide encryption key management. The new product, which is called Vormetric Key Management (VKM), extends the capabilities of the Vormetric Data Security Manager to provide key life cycle management for non-Vormetric enterprise encryption solutions. Support for third party encryption products will be phased in over time as Vormetric develops a better understanding of the customer requirements, the specific encryption solutions that VKM must manage and the scope of key management that must be provided. The first release of Vormetric Key Manager will provide the full life cycle management of keys for the following third party encryption products:

1. Oracle 11gR2 Transparent Data Encryption (Oracle TDE)
2. Microsoft SQL Server Transparent Data Encryption for SQL Server 2008 and SQL Server 2012 (MS-SQL TDE)

This document is an FAQ for the software Key Agent for Microsoft SQL Server Transparent Data Encryption.

Acronyms

- **MS-SQL**: Microsoft SQL Server
- **TDE**: Transparent Data Encryption (Microsoft SQL’s native encryption for cells and database)
- **EKM**: The SQL Server Extensible Key Management enables third-party Hardware Security module (HSM) vendors to register their modules in SQL Server TDE. When registered, SQL Server can communicate with the module using a pre-defined interface to access the encryption keys stored on HSM modules.
DEK: Database Encryption Key. Encrypts the database

HSM: Hardware Security Module. Used to store keys securely

DSM: Vormetric Data Security Manager, the management software and the user interface that is used to administer security policies, keys and access control for key agents

Security Server: The DSM packaged in an appliance form factor

Microsoft SQL Server 2008 & SQL Server 2012 TDE

1. What is Microsoft SQL Server TDE? Microsoft SQL Server 2008 and 2012 offer native encryption for database cells as well as the entire database. This native encryption is called “Transparent Data Encryption” or “TDE”. When TDE is enabled a Database Encryption Key (DEK) is created. The DEK is protected (encrypted) with an asymmetric key. The asymmetric key can be stored in the HSM for maximum security.

2. What is the Microsoft SQL Server TDE Database Encryption Key (DEK)? The DEK is the key that is used to encrypt/decrypt the Microsoft SQL Server database.

3. What is an EKM provider? EKM provider is the HSM or Key Manager vendor. This vendor distributes the library of EKM APIs that are registered with the Microsoft SQL Server database. For example, Vormetric distributes an EKM API library as a DLL. This DLL communicates with the Vormetric Key Manager for key management.

4. Where are MS SQL Server TDE encryption keys stored? Microsoft SQL Server TDE has a single encryption key for a database and this is called the Database Encryption Key (DEK). It is created by MS SQL Server, stored in the SQL database and managed by MS SQL Server. The DEK is not visible to the database or security administrator.

5. What about MS SQL Server cell keys? Vormetric Key Manager does not support key life cycle management for cell-level keys. These keys are created, managed and stored in the SQL Server.

6. How is the DEK protected? The DEK can be protected by a password, a certificate or an asymmetric key. Protecting with an asymmetric key stored in an EKM’s provider’s security appliance offers the most secure protection with separation of duties. Vormetric Key Manager is the EKM provider for SQL TDE.

7. Where is the asymmetric key that encrypts the DEK stored? The asymmetric key is stored in the EKM provider’s security appliance. Vormetric Key Management is an EKM provider.

8. Where can I learn more about Microsoft SQL Server TDE? Microsoft website has several white papers on Microsoft SQL Server TDE. A good place to start is the paper on SQL TDE and configuring an EKM provider.

Public Key Cryptography Standard (PKCS)
1. **What is PKCS?** Public Key Cryptography Standard #11 (PKCS) is a specification for interfacing with security devices that store security objects (tokens, certificates, keys, digests).
   a. Specifies Application Programming Interface (API) called “Cryptoki” in “C” language
   b. Does not specify storage format
   c. Current version is 2.20

2. **Is Vormetric implementing the PKCS#11 APIs?** Vormetric is implementing a subset of the PKCS #11 APIs necessary to manage keys and provide cryptographic services. The APIs will be available as a library. Applications such as MS SQL Server dynamically link to this library.

3. **What is the relationship between Microsoft SQL TDE, EKM provider and Vormetric PKCS#11 APIs?** Microsoft SQL Server TDE invokes the Extensible Key Management (EKM) APIs for key management using HSMs. Vormetric has implemented the EKM APIs as dynamic library of APIs. The EKM APIs in turn invoke Vormetric’s implementation of the PKCS#11 APIs.

**Vormetric Key Manager and Microsoft SQL Server TDE**

1. **How does Vormetric provide key management for Microsoft SQL Server TDE?** Vormetric provides the HSM functionality for Microsoft SQL Server TDE and encrypts the Database Encryption Key (DEK)

2. **Which Microsoft SQL TDE keys are managed by Vormetric Key Manager (VKM)?** VKM manages the asymmetric keys that protect the Database Encryption Key (DEK).

3. **What are all the software/hardware components that make up the Vormetric Microsoft SQL TDE solution?** There are three components:
   a. The EKM library of APIs
   b. The PKCS#11 library of APIs. The EKM and PKCS #11 libraries together are called “Key Agent”
   c. The Vormetric Data Security Manager (DSM)

4. **Is the Vormetric “Key Agent” different from the Vormetric Encryption Expert agent?** Yes, this is an entirely new software agent. However, it communicates with the Vormetric Data Security Manager for Microsoft SQL Server TDE Database Encryption Key (DEK) life cycle management.

5. **Can the Vormetric Key Agent co-exist with the Vormetric Encryption Expert agent?** Yes

6. **What are the types of communication exchanged between the Vormetric “Key Agent” and Vormetric Data Security Manager?** Similar to the communication between the Vormetric Encryption Expert Agent and the Data Security Manager, the following are the key communication areas:
   a. Registration (Key agent registers itself with DSM)
   b. API calls for Key Life Cycle Management (e.g. Key creation, deletion, encryption, deletion etc.)
   c. Upload audit log files

7. **Can policies be assigned to Microsoft SQL Server TDE keys?** No, there are no policies or rules associated with Microsoft SQL Server TDE keys. All key life cycle management functions are initiated by MS SQL Server 2008/MS SQL Server 2012 and completed by the Key Agent and Data Security Manager.
8. **Why aren’t earlier versions of MS SQL Server supported?** Versions of Microsoft SQL Server prior to Microsoft SQL Server 2008 did not have an API framework for supporting Hardware Security Model (HSM). Consequently, versions of MS SQL Server prior to SQL Server 2008 are not supported by Vormetric Key Management.

**Microsoft SQL Server TDE Use Cases**

1. **Enable EKM:** This is an explicitly defined step in MS-SQL to *enable* the creation of asymmetric keys to protect the Database Encryption Key (DEK). This is the first step that informs MS-SQL that an external Hardware Security Module (HSM) will be used.
2. **Create Key:** Asymmetric keys are used to protect the DEK. Create and delete use cases create and delete an asymmetric key pair.
3. **Transparent Database Encryption (TDE) with EKM:** This use case causes the DEK to be encrypted/decrypted with the asymmetric keys created and stored in the DSM.
4. **Rotate Key:** This use case causes the asymmetric keys protecting the DEK to be regenerated. In some cases this process helps meet regulatory requirements.
5. **Separation of duties:** The security administrator creates the asymmetric keys and associated attributes for use by the SQL server and provides the key name to SQL Database Administrator (DBA). The DBA uses this key to encrypt the DEK.

**Vormetric Key Agent – Audit Logging**

1. **Does the Key Agent log messages?** Yes.
2. **Where is the log file located?** The key agent log is located in the following location as:
   
   a. `C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\vorpkcs11_SYSTEM.log`

**Vormetric Data Security Manager, Key Agent and Microsoft SQL Server TDE keys**

1. **What is the role of the Vormetric Data Security Manager (DSM)?** The Vormetric Data Security Manager provides the web services for encryption key management. The Vormetric Key Agent, acting on behalf of Microsoft SQL Server TDE consumes the DSM web services for Microsoft SQL Server TDE key management and encryption.
2. **Are the Microsoft SQL Server TDE keys stored in the DSM?** Yes. The Vormetric DSM stores the asymmetric keys that protect the DEK. Other keys used by MS SQL Server for cell and database encryption can also be created and stored in the Vormetric DSM.
3. **Do the Microsoft SQL Server TDE asymmetric keys that protect the DEK leave the DSM?** No, the asymmetric keys protecting the DEK never leave the DSM. However, it is possible that the public key of the asymmetric key pair can be exported out of the DSM.
4. **How are Microsoft SQL Server TDE cell and database keys encrypted/decrypted?** Microsoft SQL TDE keys are encrypted/decrypted with the DEK. The DEK is stored in the SQL database.
5. Can the Data Encryption Key (DEK) be “Cached on host” (key agent)? No. The DEK is already stored (cached) in the SQL Server database. Neither the Key Agent nor the Vormetric DSM has any knowledge of the DEK.

6. Is the Microsoft SQL Server TDE Data Encryption Key (DEK) treated differently than the Vormetric Encryption Expert Keys? From the Vormetric DSM point of view, a key is a key and no distinction is made by the two.

7. Can the Microsoft SQL Server TDE Data Encryption Key be specified in a policy for Vormetric Encryption Expert agent? No. The Vormetric DSM has no knowledge of the DEK.

8. Can the Microsoft SQL Server TDE Data Encryption Key be deleted from the Vormetric DSM? The Vormetric DSM has no knowledge of the DEK. The asymmetric keys that protect the DEK cannot be deleted.

9. Does the Vormetric DSM HA make the Key Agent highly available? No. If the primary Vormetric DSM serving the Key Agent dies, the Key Agent can communicate with a failover DSM in the cluster for read only operations.

Licensing

1. Is the Key Agent licensed? Yes, the Vormetric Key Agent, much like the Vormetric Encryption Expert agent is licensed and priced separately. Please consult a Vormetric sales representative for pricing information.

2. Is the Vormetric DSM for Key Management licensed? No. Although, the pricing and features available with the Vormetric DSM are being changed for Vormetric Encryption and Vormetric Key Management V5.


## Vormetric Key Agent - Supported platforms

The Vormetric Key Agent for Microsoft SQL TDE is supported on the following platforms:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Processor Architecture</th>
<th>Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 Standard R1</td>
<td>32-bit x86</td>
<td>SQL Server 2008 (32-bit)</td>
</tr>
<tr>
<td>Windows 2008 Enterprise R1</td>
<td>32-bit x86</td>
<td>SQL Server 2008 (64-bit)</td>
</tr>
<tr>
<td>Windows 2008 DataCenter R1</td>
<td>32-bit x86_64</td>
<td>SQL Server 2008 R2 (32-bit)</td>
</tr>
<tr>
<td>Windows 2008 Standard R2</td>
<td>64-bit x86</td>
<td>SQL Server 2008 SP1 (64-bit)</td>
</tr>
<tr>
<td>Windows 2008 Enterprise R2</td>
<td>64-bit x86_64</td>
<td>SQL Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td>Windows 2008 DataCenter R2</td>
<td>64-bit x86_64</td>
<td>SQL Server 2012 (64-bit)</td>
</tr>
</tbody>
</table>

## References

1. Understanding MS-SQL TDE
2. Database Encryption in SQL Server 2008 Enterprise Edition
3. Configuring an EKM provider

Copyright © 2012 Vormetric, Inc. All Rights Reserved.

This document is provided for informational purposes only and the document content is subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Vormetric specifically disclaims
any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.

Vormetric is a registered trademark of Vormetric, Inc. in the U.S.A. and certain other countries. All other trademarks or registered trademarks, product names, company names and logos cited are the property of their respective owners.