Document Information

<table>
<thead>
<tr>
<th>Product Version</th>
<th>1.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Part Number</td>
<td>007-013897-001</td>
</tr>
<tr>
<td>Release Date</td>
<td>21 November 2018</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rev. A</td>
<td>17 August 2017</td>
<td>For initial release 1.1.0</td>
</tr>
<tr>
<td>Rev. B</td>
<td>19 September 2017</td>
<td>For release 1.1.1</td>
</tr>
<tr>
<td>Rev. C</td>
<td>14 November 2017</td>
<td>For release 1.2</td>
</tr>
<tr>
<td>Rev. D</td>
<td>05 February 2018</td>
<td>For release 1.3</td>
</tr>
<tr>
<td>Rev. E</td>
<td>02 March 2018</td>
<td>For HSM on Demand release 1.3</td>
</tr>
<tr>
<td>Rev. F</td>
<td>05 April 2018</td>
<td>For release 1.4</td>
</tr>
<tr>
<td>Rev. G</td>
<td>07 May 2018</td>
<td>For HSM on Demand release 1.4</td>
</tr>
<tr>
<td>Rev. H</td>
<td>10 June 2018</td>
<td>For release 1.5</td>
</tr>
<tr>
<td></td>
<td>12 September 2018</td>
<td>For release 1.6</td>
</tr>
<tr>
<td></td>
<td>21 November 2018</td>
<td>For release 1.7</td>
</tr>
</tbody>
</table>

Trademarks and Copyrights

Copyright 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.
The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms’ resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Gemalto.
# SafeNet Data Protection on Demand 1.7

**MICROSOFT SQL SERVER INTEGRATION GUIDE**

## Contents

**Overview**
- Third Party Application Details .......................................................... 5
- Supported Platforms .............................................................................. 5
- About Microsoft SQL ................................................................................ 5
- About Microsoft SQL Server High Availability (Always On) ...................... 6
- Support for Higher-length Asymmetric Keys ........................................... 6

**Preparing for the integration**
- Set up Luna EKM .................................................................................. 7
- Set up SQL Server .................................................................................... 7
- Provision HSMoD Service ......................................................................... 7
  - Adding a Service ................................................................................... 7
  - Adding a Service Client ......................................................................... 8
  - Initializing the HSM ............................................................................... 9
- Constraints on HSMoD Services ............................................................... 10

**Integrating Microsoft SQL Server or SQL Server High Availability (Always On) Group with HSM on Demand Service** ........................................... 11
- Enabling the Luna EKM Provider Option ................................................. 11
- Registering the Luna EKM Provider Option ............................................. 12
- Setting up the Credential for Luna EKM Provider .................................... 13
- Creating the Always On Availability Group ............................................ 13
- Using the Luna EKM Provider Option ..................................................... 13
- Creating Symmetric Key Encrypted by Asymmetric Key on an HSM on Demand Service .......................................................... 17
- Enabling Transparent Data Encryption using Asymmetric Key on HSM on Demand service ......................................................... 18
- Rotating Keys for Transparent Data Encryption ...................................... 19
- Migrating from SQL EKM to Luna EKM ................................................ 20
- Adding an Encrypted Database to the Availability Group ..................... 21
- Using Extensible Key Management on a SQL Server Failover Cluster .......... 22
Overview

SQL Server enables use of an HSM on Demand (HSMoD) Service for storage of keys and cryptographic operations such as key creation, deletion, encryption, and decryption, by using the Extensible Key Management (EKM) feature. Data can be encrypted by using encryption keys that only the database user has access to on the external EKM/HSM module. SafeNet provides Luna EKM which includes the EKM Provider Library for the HSM on Demand Service that can be used to setup Extensible Key Management (EKM) for SQL Server and facilitate the integration with the HSM on Demand Service.

We recommend you familiarize yourself with SQL server operations and basic HSM concepts to make full use of the You must have basic knowledge of using SQL Server and HSM concepts.

This document contains the following sections:
> "Preparing for the integration" on page 7
> "Integrating Microsoft SQL Server or SQL Server High Availability (Always On) Group with HSM on Demand Service" on page 11

This overview contains the following topics:
> "Third Party Application Details" below
> "Supported Platforms" below
> "About Microsoft SQL" below
> "About Microsoft SQL Server High Availability (Always On)" on the next page

Third Party Application Details

This integration guide uses the following third party applications:
> Microsoft SQL

Supported Platforms

The following platforms are tested with HSMoD Service:
> Windows Server 2016
> Windows Server 2012R2

About Microsoft SQL

Microsoft SQL Server is a database platform for large-scale online transaction processing (OLTP), data warehousing, and e-commerce applications; it is also a business intelligence platform for data integration, analysis, and reporting solutions.

The following diagram demonstrates the relationship between the database master key and the HSM devices in a Microsoft SQL configuration:
About Microsoft SQL Server High Availability (Always On)

The Always On Availability Groups feature is a high-availability and disaster recovery solution that provides an enterprise-level alternative to database mirroring. Introduced in SQL Server 2012, Always On Availability Groups maximize the availability of a set of user databases for an enterprise. An availability group supports a failover environment for a discrete set of user databases, known as availability databases that fail over together. An availability group supports a set of read-write primary databases and one to eight sets of corresponding secondary databases. Optionally, secondary databases can be made available for read-only access and/or backup operations.

NOTE The HSM on Demand Client and Luna EKM must be setup on all nodes in the SQL server configuration that will be added to the Always On availability group. All nodes must be registered with the same [Undefined variable Default.slot]] on the HSM on Demand Service.

Support for Higher-length Asymmetric Keys

HSM on Demand services can support up to five 4096-bit RSA keys. Longer bit RSA keys increase the security of cryptographic operations.

CAUTION! The integration testing identified an issue in TDE when encrypting the DEK using an RSA_4096 key. The issue has been reported to Microsoft technical support and we are awaiting a resolution. At this time, we recommend using a maximum RSA key length of 3072-bit.
Preparing for the integration

Before you proceed with the integration, ensure you have completed the following:

> "Set up Luna EKM" below
> "Set up SQL Server" below
> "Provision HSMoD Service" below

Set up Luna EKM

LunaEKM includes a command line configuration utility LunaEKMConfig that is used to register the Luna EKM. This command line utility is available in the LunaEKM installation folder. It provides command to register slots, view slots and to configure log settings.

Run the following commands from the LunaEKMConfig directory.

1. RegisterSlot - register or edit the slot for the LunaEKM to use.
2. ViewSlots - View a list of the slots and the HSM configured with this client.
3. LogSettings - Configure log settings for LunaEKM

```
LogLevel (NONE=0,INFO=1,DEBUG=2): <LogLevel>
LogFile name: <Name and location of LogFile>
```

Set up SQL Server

SQL Server must be installed on the target machine to carry out the integration process. If you are configuring an Always On availability group all nodes in the configuration require WSFC.

For a detailed installation procedure of SQL Server, refer to the Microsoft SQL Server online documentation.

Provision HSMoD Service

The HSM on Demand Service provides your client machine with access to an HSM application partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

You must provision your HSM on Demand service by adding the service, downloading the service client package and initializing the HSM. Provisioning your HSM on Demand service entails:

> "Adding a Service" below
> "Adding a Service Client" on the next page
> "Initializing the HSM" on page 9

Adding a Service

1. Under the Services tab, select the Add New Service page. Click Deploy on the service tile for the service you wish to add.
NOTE Click **Deploy** on the HSM on Demand Service tile for your integration.

2. Review the "Terms of Services DPoD." Enable the **I have read and accept the Terms of Service above** check box and then click **Next**.

3. On the **Add <service_type> Service** page, enter a name for the Service in the **Service Name** field. You can optionally allow non-FIPS approved algorithms by selecting the **Allow non-FIPS approved algorithms** check box. Click **Next**.

**CAUTION!** You cannot alter the FIPS setting after creating the service. You must decide if the service should allow or disallow non-FIPS approved algorithms before clicking **Finish** in the next step.

4. Review the configuration summary page. If acceptable, click **Finish**. If you would like to make changes to the configuration, click **Go Back**.

When completed, the new service is listed under My Services and a **Create Service Client** window displays.

5. Click **Create Service Client**.

**Adding a Service Client**

1. In the **Create Service Client** window enter a name for the service client in the **Service Client Name** field.

**NOTE** If the **Create Service Client** window is not available, navigate to the **Services** tab and click the name of the Service you would like to generate a client for in the **My Services** tab. On the Service Details page, click **New Service Client**.

2. Select **Create Service Client**.

A new HSM service client package is created and provided for downloading on your client system.

**NOTE** The HSM service client package is a zip file that contains system information needed to connect your client system to an existing HSM on Demand service. The HSM service client package should download immediately on creation. If it does not, or you lose access to your HSM service client package it can be accessed or reacquired through the **My Services** table.

3. Transfer the service client package to your client system. You can use SCP, PSCP, WinSCP, FTPS, or any other secure file transfer tool.

4. Unzip the service client package.

   For Linux, enter:
   ```
   unzip <service_client_package>.zip
   ```

   For Windows, using the Windows GUI or an unzip tool unzip the file:
   ```
   <service_client_package>.zip
   ```
Preparing for the integration

5. Extract the cvclient-min file.

   NOTE Extract the cvclient-min file in the directory where you extracted the <service_client_package>.zip. Do not extract to a new cvclient-min directory.

For Linux, untar the cvclient-min.tar

tar xvf cvclient-min.tar

For Windows, unzip the cvclient-min.zip.

6. Set the environment variable.

   For Linux, execute:
   
source ./setenv

   For Windows, right click setenv.cmd and select Run as Administrator.

   NOTE If you encounter the error dll load failed with GetLastError() 126 move the contents of the cvclient_min folder up one directory and execute setenv.

7. Start LunaCM.

   For Linux, execute the following from the directory where you extracted the cvclient-min.tar file.
   
   ./bin/64/lunacm

   For Windows, execute the following from the directory where you unzipped the cvclient-min.zip file.
   
   lunacm

Initializing the HSM

1. Set the active slot to the service partition.

   lunacm:>slot set -slot <slot_number>

   NOTE Execute slot list in LunaCM to identify the slot number associated with your service.

2. Initialize the application partition. During this process you will create the partition’s Security Officer (SO), set the SO password, and specify the cloning domain.

   lunacm:> partition init -label <service_label>

3. Optional: If you wish to transfer key material to or from a PED-authenticated Luna partition, you initialize the SafeNet Data Protection On Demand partition using the red PED domain key.

   a. For DPoD deployments, contact customer support to obtain the necessary PED drivers so that your HSM client can communicate with the PED.
b. Attach the PED locally to the client computer, insert the red cloning domain PED key, and initialize the partition, including the option to set the cloning domain from the red PED key. Execute:

```bash
lunacm:> partition init -label <cryptovisor_partition_label> -importpeddomain
```

4. Log in as the partition’s Security Officer:

```bash
lunacm:> role login -name Partition SO
```

5. Initialize the Crypto Officer role:

```bash
lunacm:> role init -name Crypto Officer
```

6. Log out of the partition Security Officer role and log in as the Crypto Officer.

```bash
lunacm:> role logout
lunacm:> role login -name Crypto Officer
```

7. You must change the Crypto Officer password immediately on the initial log in. Failure to due so will result in a password error on subsequent logins.

```bash
lunacm:> role changepw -name Crypto Officer
```

8. Initialize the Crypto User role:

```bash
lunacm:> role init -name Crypto User
```

9. Log out of the partition Crypto Officer role and log in as the Crypto User.

```bash
lunacm:> role logout
lunacm:> role login -name Crypto User
```

10. You must change the Crypto User password immediately on the initial log in. Failure to do so will result in a password error on subsequent logins.

```bash
lunacm:> role changepw -name Crypto User
```

This completes initializing the HSM on Demand Service. The Crypto Officer and Crypto User roles can now be used to integrate applications with the HSMoD service to perform cryptographic operations.

**Constraints on HSMoD Services**

Please take the following limitations into consideration when integrating your application software with an HSM on Demand Service.

**HSM on Demand Service in FIPS mode**

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the **Mechanism List** in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

### Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use **slot list** to determine which slot numbers are in use by which HSMoD service.
Integrating Microsoft SQL Server or SQL Server High Availability (Always On) Group with HSM on Demand Service

This document contains detailed instructions and procedures to integrate Microsoft SQL Server with an HSM on Demand Service.

This integration contains the following topics:

- "Enabling the Luna EKM Provider Option" below
- "Registering the Luna EKM Provider Option" on the next page
- "Setting up the Credential for Luna EKM Provider" on page 13
- "Creating the Always On Availability Group" on page 13
- "Using the Luna EKM Provider Option" on page 13
- "Creating Symmetric Key Encrypted by Asymmetric Key on an HSM on Demand Service" on page 17
- "Enabling Transparent Data Encryption using Asymmetric Key on HSM on Demand service" on page 18
- "Rotating Keys for Transparent Data Encryption" on page 19
- "Migrating from SQL EKM to Luna EKM" on page 20
- "Adding an Encrypted Database to the Availability Group" on page 21
- "Using Extensible Key Management on a SQL Server Failover Cluster" on page 22

NOTE Extensible Key Management is disabled by default.

Enabling the Luna EKM Provider Option

To use the Luna EKM provider you must enable the Luna EKM provider option on the SQL Server. The Luna EKM software grants access to the Luna EKM Provider software in the form of the EKM library (LunaEKM.dll) to integrate the HSM on Demand Service with SQL Server. The Luna EKM provider can be used if the EKM provider option is enabled on the SQL server. This feature is only available on the Enterprise, Developer, and Evaluation editions of SQL server.

To enable the Luna EKM Provider Option

Use the `sp_configure` command to enable the Luna EKM provider option on both the SQL server nodes. The following is an example procedural set on enabling the Luna EKM provider option.

1. Open the SQL Server Management Studio.
2. Connect to the SQL Server.
3. Open a Query window and execute the following:

   ```sql
   sp_configure 'show advanced', 1
   GO
   ```
Integrating Microsoft SQL Server or SQL Server High Availability (Always On) Group with HSM on Demand

RECONFIGURE
GO
sp_configure 'EKM provider enabled', 1
GO
RECONFIGURE
GO

NOTE  Note: The sp_configure command can only be run in an Enterprise, Developer or Evaluation edition of MS SQL.

Registering the Luna EKM Provider Option

To setup the Luna EKM provider, Luna EKM Software must be installed and needs to be registered with the SQL Server. Follow the steps below to register the provider on all SQL Server nodes.

To register the Luna EKM Provider Option

Create a new cryptographic provider file that will use the Luna EKM provider.

1. Open the SQL Server Management Studio.
2. Connect to the SQL Server.
3. Open a Query window and execute the following:

   CREATE CRYPTOGRAPHIC PROVIDER <name_of_cryptographic_provider>
   FROM FILE = '<location_of_LUNA_EKM_Provider_Library>'

4. View the list of EKM providers:

   SELECT [provider_id]
   ,[name]
   ,[guid]
   ,[version]
   ,[dll.path]
   ,[is_enabled]
   FROM [model].[sys].[cryptographic_providers]

5. View the provider properties:

   SELECT [provider_id],[guid],[provider_version]
   ,[sqlcrypt_version]
   ,[friendly_name]
   ,[authentication_type]
   ,[symmetric_key_support]
   ,[symmetric_key_persistance]
   ,[symmetric_key_export]
   ,[symmetric_key_import]
   ,[asymmetric_key_support]
   ,[asymmetric_key_persistance]
   ,[asymmetric_key_export]
   ,[asymmetric_key_import]
   FROM [master].[sys].[dm_cryptographic_provider_properties]
Setting up the Credential for Luna EKM Provider

You must create a CREDENTIAL for the Luna EKM provider. You must then map that CREDENTIAL to the SQL User or login to use the Luna EKM provider option. Follow the steps below to create the CREDENTIAL and map it to the SQL User on all SQL Server nodes.

TIP A CREDENTIAL is used to access external SQL Server resources such as the HSM on Demand Service.

To setup Credential for Luna EKM Provider

Create and map the CREDENTIAL to the Luna EKM Provider.

1. Open a Query window and execute the following to create the CREDENTIAL:

   CREATE CREDENTIAL <name_ofCredential> WITH IDENTITY='EKM_user', SECRET='HSM_partition_password'
   FOR CRYPTOGRAPHIC PROVIDER LunaEKMProvider

2. Map the Luna EKM Credential with SQL User or Login.

   ALTER LOGIN [Domain\Login Name]
   ADD CREDENTIAL <name_ofCredential>

NOTE The EKM session must be reopened if the user changes the HSM service, the client machine is deleted from the HSM on Demand Service, or the machine suffers a network disconnection.

Creating the Always On Availability Group

If you are configuring a Microsoft SQL Always On availability group you must complete this process. If you are not configuring an Always on Availability Group proceed to “Using the Luna EKM Provider Option” below.

Open the Microsoft SQL Server Management Studio on the primary node and create a database. Take a complete backup of that database on a location that is accessible by all SQL Server nodes. Open the Always On Availability Group Creation wizard and follow the instructions to create an Always on Availability Group.

After successful configuration, the dashboard displays all of the participating nodes.

Refer to the Microsoft Online Documentation for detailed procedures and prerequisites for creating the Always On Availability Group.

Using the Luna EKM Provider Option

The Luna EKM provider can be used to create/drop symmetric and asymmetric keys to/from the service and can perform encryption/decryption using these keys.

The Luna EKM Provider can be used to generate and manipulate the following:

> "Symmetric Keys on an HSM on Demand Service" on the next page
> "Asymmetric Keys on an HSM on Demand Service" on page 15
Symmetric Keys on an HSM on Demand Service
The following types of symmetric keys can be generated on the HSM on Demand Service using the SQL Server:

- RC2
- RC4*
- RC4_128*
- DES
- Triple_DES
- AES_128
- AES_192
- AES_256
- RC4_128*
- Triple_DES_3KEY
- AES_192
- AES_256

*deprecated in SQL Server 2012

To create symmetric keys using the Luna EKM Provider
You can create symmetric keys by executing the following command from the SQL Query window. In the following example the AES algorithm is used to generate a symmetric key.

1. CREATE SYMMETRIC KEY SQL_EKM_AES_256_Key
   FROM Provider LunaEKMPProvider
   WITH ALGORITHM = AES_256,
   PROVIDER_KEY_NAME = 'EKM_AES_256_Key',
   CREATION_DISPOSITION=CREATE_NEW

**NOTE** Once a key is created on the HSM on Demand Service, it can be accessed, by name, from the SQL Server. In the above example, SQL_EKM_AES_256_Key is the unique name of the key in the SQL Server. Using this key name will use the key on the HSM for encrypt and decrypt operations.

To view symmetric keys using the Luna EKM Provider
You can view symmetric keys by executing the following command from the SQL Query window.

1. SELECT * FROM [master].[sys].[symmetric_keys]

To encrypt with symmetric keys using the Luna EKM Provider
You can encrypt tables in the database using the Luna EKM Provider key stored on the HSM on Demand Service.

1. Create a test table in the database with fields. For example:
   Create Table test(
   id numeric(10),
   name varchar (50),
   data varchar (max),
   )

2. Execute the following command to insert encrypted content into the table.
   INSERT INTO dbo.test
   values( 1,'some text',
   EncryptByKey(Key_GUID('SQL_EKM_AES_256_Key'), '<text_to_beencrypted>'))
To decrypt with symmetric keys using the Luna EKM Provider

You can decrypt tables in the database using the Luna EKM Provider key stored on the HSM on Demand Service. To decrypt the table contents that were encrypted in the last procedural set, open an SQL Query window and execute the following:

1. SELECT id,name,CONVERT(varchar(MAX),
   DecryptByKey(data))
   FROM dbo.test where id =1

2. If you are configuring an Always On availability group, execute the above command on the secondary node and verify the output is the same as the output received on the primary node.

To drop symmetric keys using the Luna EKM Provider

You can drop symmetric keys using the Luna EKM Provider. The following example command will drop the keys from both the SQL Server and the HSM on Demand Service.

1. DROP SYMMETRIC KEY SQL_EKM_AES_256_Key REMOVE PROVIDER KEY

   **NOTE** We do not recommend dropping keys when operating in an Always On availability group or when running Always Encrypted

Asymmetric Keys on an HSM on Demand Service

The following types of asymmetric keys can be generated on the HSM on Demand Service using the SQL Server:

- RSA-512
- RSA_1024
- RSA_2048
- RSA_3072
- RSA_4096

To create asymmetric keys using the Luna EKM Provider

You can create asymmetric keys by executing the following command from the SQL Query window. In the following example the RSA_2048 algorithm is used to generate an asymmetric key.

1. CREATE ASYMMETRIC KEY SQL_EKM_RSA_2048_KEY
   FROM Provider LunaEKMPProvider
   WITH ALGORITHM = RSA_2048,
   PROVIDER_KEY_NAME = 'EKM_RSA_2048_Key',
   CREATION_DISPOSITION=CREATE_NEW
NOTE Once a key is created on the HSM on Demand Service, it can be accessed, by name, from the SQL Server. In the above example, SQL_EKM_RSA_2048_Key is the unique name of the key in the SQL Server. Using this key name will use the key on the HSM for encrypt and decrypt operations.

To view asymmetric keys using the Luna EKM Provider

You can view asymmetric keys by executing the following command from the SQL Query window.

1. SELECT * FROM [master].[sys].[asymmetric_keys]

To encrypt with asymmetric keys using the Luna EKM Provider

You can encrypt tables in the database using the Luna EKM Provider key stored on the HSM on Demand Service.

1. Create a test table in the MASTER database with fields. For example:
   
   Create Table test(
   id numeric(10),
   name varchar (50),
   data varchar (max),)

2. Execute the following command to encrypt content and insert it into the table.

   INSERT INTO dbo.test
   values( 1,'some text',
   EncryptByAsymKey(AsymKey_Id('SQL_EKM_RSA_2048_Key'), '<text_to_be_encrypte>'))

To decrypt with asymmetric keys using the Luna EKM Provider

You can decrypt tables in the database using the Luna EKM Provider key stored on the HSM on Demand Service. To decrypt the table contents that were encrypted in the last procedural set, open an SQL Query window and execute the following:

1. SELECT id,name,CONVERT (varchar (MAX),
   DecryptByAsymKey (AsymKey_Id ('SQL_EKM_RSA_2048_Key', data))
   FROM dbo.test where id =1

2. If you are configuring an Always On availability group, execute the above command on the secondary node and verify the output is the same as the output received on the primary node.

To drop asymmetric keys using the Luna EKM Provider

You can drop symmetric keys using the Luna EKM Provider. The following example command will drop the keys from both the SQL Server and the HSM on Demand Service.

1. DROP ASYMMETRIC KEY SQL_EKM_RSA_2048_Key REMOVE PROVIDER KEY
Creating Symmetric Key Encrypted by Asymmetric Key on an HSM on Demand Service

You can encrypt the symmetric keys shared by the nodes in the standalone or cluster configuration using an asymmetric key. This increases the security of the symmetric key.

To create a symmetric key encrypted by an asymmetric key

1. Execute the following command from an SQL Query window.

   ```sql
   Create SYMMETRIC KEY key1
   WITH ALGORITHM = AES_256
   ENCRYPTION BY Asymmetric Key SQL_EKM_RSA_2048_Key;
   ```

   **NOTE** SQL_EKM_RSA_2048 Key is an existing asymmetric key on the HSM on Demand Service. For more information about generating the asymmetric key see "To create asymmetric keys using the Luna EKM Provider" on page 15.

2. Open the symmetric key.

   ```sql
   OPEN SYMMETRIC KEY key1 DECRYPTION BY Asymmetric Key SQL_EKM_RSA_2048_key;
   ```

3. Create a test table in the MASTER database with fields.

   ```sql
   Create Table test(
   id numeric(10),
   name varchar (50),
   data varchar (max),
   )
   ```

4. Encrypt data using the symmetric key.

   ```sql
   INSERT INTO dbo.test
   values ( 1,'some text',
   EncryptByKey(KEY_GUID('key1'),'<text_to_be_encrypted>'))
   ```

5. Decrypt the data using the symmetric key.

   ```sql
   SELECT id,name,CONVERT(varchar(MAX),
   DecryptByKey(data))
   FROM dbo.test where id =1
   ```

6. Close the symmetric key.

   ```sql
   CLOSE SYMMETRIC KEY key1
   ```

7. If you are configuring an Always On availability group, execute steps 2-5 on the secondary replica and verify that the output is the same as the output on the primary replica.
Enabling Transparent Data Encryption using Asymmetric Key on HSM on Demand service

You can enable Transparent Data Encryption (TDE) using an asymmetric key stored on the HSM on Demand service.

**To enable TDE using Asymmetric key on HSMoD service**

1. Create an asymmetric key using the LunaEKM provider.
   ```sql
   Use master;
   CREATE ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE_Rot
   FROM Provider LunaEKMProvider
   WITH ALGORITHM = RSA_2048,
   PROVIDER_KEY_NAME = 'EKM_RSA_2048_Key_TDE_Rot',
   CREATION_DISPOSITION=CREATE_NEW
   ```

2. Create a CREDENTIAL for Luna EKM provider
   ```sql
   CREATE CREDENTIAL <name_of_credential>
   WITH IDENTITY='EKM_user', SECRET='<service_password>'
   FOR CRYPTOGRAPHIC PROVIDER LunaEKMProvider
   ```

3. Create a login based on the recently created asymmetric key.
   ```sql
   CREATE LOGIN <Name of login>
   FROM ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE_Rot;
   ```

4. Map the recently created credential to the recently created login.
   ```sql
   ALTER LOGIN <Name of Login>
   ADD CREDENTIAL <Name of credential>;
   ```

5. Create a database encryption key.
   ```sql
   CREATE DATABASE TDE;
   Use tde;
   CREATE DATABASE ENCRYPTION KEY
   WITH ALGORITHM = AES_256
   ENCRYPTION BY SERVER ASYMMETRIC KEY SQL_EKM_RSA_@)$$*_KEY_TDE;
   ```

6. Enable Transparent Data Encryption
   ```sql
   ALTER DATABASE TDE
   SET ENCRYPTION ON;
   ```

7. Query the status of database encryption and the completion percentage.
   ```sql
   SELECT DB_NAME (e.database_id) AS DatabaseName, e.database_id,
   e.encryption_state,
   CASE e.encryption_state
   WHEN 0 THEN 'No database encryption is present, no encryption'
   WHEN 1 THEN 'Uncrypted'
   WHEN 2 THEN 'Encryption in progress'
   WHEN 3 THEN 'Encrypted'
   WHEN 4 THEN 'Key change in progress'
   WHEN 5 THEN 'Decryption in progress'
   ```

**NOTE** Database encryption operations cannot be executed on master, model, tempdb, msdb, or resource databases.
END AS encryption_state_desc,
c.name,
e.percent_complete
FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.asymmetric_keys AS c
ON e.encryptor_thumbprint = c.thumbprint

Rotating Keys for Transparent Data Encryption

We recommend updating your Transparent Data Encryption security keys regularly.

To rotate keys for TDE

1. Generate an asymmetric key using the Luna EKM provider.

   Use master;
   CREATE ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE_Rot
   FROM Provider LunaEKMProvider
   WITH ALGORITHM = RSA_2048,
   PROVIDER_KEY_NAME = 'EKM_RSA_2048_Key_TDE_Rot',
   CREATION_DISPOSITION=CREATE_NEW

2. If you are using configuring an Always On availability group, create the same asymmetric key using Luna EKM provider on the secondary node. If you are not configuring an Always On availability group, skip this step.

   Use master;
   CREATE ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE_Rot
   FROM Provider LunaEKMProvider
   WITH PROVIDER_KEY_NAME = 'EKM_RSA_2048_Key_TDE_Rot',
   CREATION_DISPOSITION=OPEN_EXISTING

3. Create a credential for the Luna EKM provider.

   CREATE CREDENTIAL <name_of_credential>
   WITH IDENTITY='<EKM_user>', SECRET='<service_password>'
   FOR CRYPTOGRAPHIC PROVIDER LunaEKMProvider

4. Create a login based on the recently created asymmetric key.

   CREATE LOGIN <Name of login>
   FROM ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE_Rot;

5. Map the credential to the login.

   ALTER LOGIN <Name of Login>
   ADD CREDENTIAL <Name of credential>;

6. If you are configuring an Always On availability group, repeat steps 2-5 for all secondary nodes in the configuration. You need to create the same key, credential and login in the master database of all the secondary nodes to access the encrypted tables created in the database on the primary.

7. Enable Transparent Database Encryption Key Rotation.

   Use tde;
   ALTER DATABASE ENCRYPTION KEY
   REGENERATE
   WITH ALGORITHM = AES_128
   ALTER DATABASE ENCRYPTION KEY
   ENCRYPTION BY SERVER ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE_Rot;
   go
8. Execute the following command to query the status of database encryption, the status of the TDE key change, and the tablespace encryptions percentage of completion.

```sql
SELECT DB_NAME (e.database_id) AS DatabaseName,
       e.database_id,
       e.encryption_state,
       CASE e.encryption_state
           WHEN 0 THEN 'No database encryption key present, no encryption'
           WHEN 1 THEN 'Unencrypted'
           WHEN 2 THEN 'Encryption in progress'
           WHEN 3 THEN 'Encrypted'
           WHEN 4 THEN 'Key change in progress'
           WHEN 5 THEN 'Decryption in progress'
       END AS encryption_state_desc,
       c.name,
       e.percent_complete
FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.asymmetric_keys AS c
ON e.encryptor_thumbprint = c.thumbprint
```

**Migrating from SQL EKM to Luna EKM**

If you enable Transparent Data Encryption for any database using the SQL EKM and desire to migrate TDE from SQL EKM to Luna EKM. Previously, the database master key is generated in SQL and encrypted by a certificate or asymmetric key. Now, you can generate a new database master key encrypted by an asymmetric key generated on an HSM on Demand service.

To generate a new database master encryption key encrypted by an asymmetric key generated on the HSM on Demand Service.

1. Decrypt the database.
   ```sql
   USE master;
   ALTER DATABASE <database_name>
   SET ENCRYPTION OFF;
   GO
   ```

2. Take a backup of the database and transaction logs. When the backup is completed, restart the SQL database.

3. Generate an asymmetric key using the Luna EKM provider.
   ```sql
   USE master;
   CREATE ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_AW
   FROM Provider LunaEKMPROvider
   WITH ALGORITHM = RSA_2048,
   PROVIDER_KEY_NAME = 'EKM_RSA_2048_Key_AW',
   CREATION_DISPOSITION=CREATE_NEW
   ```

4. Create a credential for the Luna EKM provider.
   ```sql
   CREATE CREDENTIAL <credential_name>
   WITH IDENTITY='<EKM_user>', SECRET='<HSM_partition_password>'
   FOR CRYPTOGRAPHIC PROVIDER LunaEKMPROvider
   ```

5. Created a login based on the recently created asymmetric key.
   ```sql
   CREATE LOGIN <login_name>
   FROM ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_AW;
   ```
6. Map the credential to the login.

   ALTER LOGIN <login_name>
   ADD CREDENTIAL <credential_name>;

7. Create a database encryption key.

   USE <database_name>
   CREATE DATABASE ENCRYPTION KEY
   WITH ALGORITHM = AES_256
   ENCRYPTION BY SERVER ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_AW;

8. Enable Transparent Data Encryption.

   ALTER DATABASE <database_name>
   SET ENCRYPTION ON;

9. Query the status of database encryption.

   SELECT DB_NAME(e.database_id) AS DatabaseName,
   e.database_id, e.encryption_state,
   CASE e.encryption_state
   WHEN 0 THEN 'No database encryption key present, no encryption'
   WHEN 1 THEN 'Unencrypted'
   WHEN 2 THEN 'Encryption in progress'
   WHEN 3 THEN 'Encrypted'
   WHEN 4 THEN 'Key change in progress'
   WHEN 5 THEN 'Decryption in progress'
   END AS encryption_state_desc,
   c.name,
   e.percent_complete
   FROM sys.dm_database_encryption_keys AS e
   LEFT JOIN master.sys.asymmetric_keys AS c
   ON e.encryptor_thumbprint = c.thumbprint

Adding an Encrypted Database to the Availability Group

If you are configuring an Always On availability group, you need to complete this procedural set for each secondary node in the availability group. If you are completing the base HSM on Demand Service integration with Microsoft SQL server, proceed to "Using Extensible Key Management on a SQL Server Failover Cluster" on the next page.

We recommend taking a complete backup of the already encrypted database. Copy the file to a shared location that is accessible by all the secondary nodes.

1. Open the SMS on the primary node.

2. Add the database to the availability group.

   use master;
   ALTER AVAILABILITY GROUP <availability_group> ADD DATABASE <database_name>;
   GO

   **NOTE** The above command adds the database to the availability group, but it is still unavailable on the secondary replica. To synchronize the database you must restore the database on the secondary replica.
3. On the secondary replica, restore the database from the backup location using the ‘RESTORE WITH NORECOVERY’ option.

4. Add the database to the secondary replica.
   
   ```
   use master;
   ALTER DATABASE <database_name> SET HADR AVAILABILITY GROUP = <availability_group>;
   ```

5. Execute the following command to query the status of database encryption
   
   ```
   SELECT DB_NAME(e.database_id) AS DatabaseName, 
   e.database_id, 
   e.encryption_state, 
   CASE e.encryption_state 
   WHEN 0 THEN 'No database encryption key present, no encryption' 
   WHEN 1 THEN 'Unencrypted' 
   WHEN 2 THEN 'Encryption in progress' 
   WHEN 3 THEN 'Encrypted' 
   WHEN 4 THEN 'Key change in progress' 
   WHEN 5 THEN 'Decryption in progress' 
   END AS encryption_state_desc, 
   c.name, 
   e.percent_complete 
   FROM sys.dm_database_encryption_keys AS e 
   LEFT JOIN master.sys.asymmetric_keys AS c 
   ON e.encryptor_thumbprint = c.thumbprint
   ```

---

**Using Extensible Key Management on a SQL Server Failover Cluster**

This section focuses on the preparation of the environment for 2-node SQL Server Cluster in Windows Server 2008 R2.

1. Refer to the SQL Server Documentation for detailed procedures on installing a failover cluster. To set up a shared storage disk for the SQL server, refer to the configuration procedures for a shared storage solution.

   **NOTE** We recommend you plan the size of the shared storage around the number of certificates that will be enrolled.

2. When the cluster is operational, install the SafeNet Luna Network HSM client on both nodes.
3. Configure and setup the appliance on both the nodes. Register the same service to both the nodes of the SQL Server Cluster.
4. Install the Luna EKM client on both the nodes.
5. Configure the Luna EKM provider on both the nodes.
6. Register the Luna EKM provider on the primary node.
7. Setup the credential on the primary node.
8. Create some keys using the Luna EKM provider on the primary node.
9. Create a database table and encrypt some columns using the Luna EKM provider on the primary node.
10. Shutdown the primary node.
11. Log in to the secondary node and decrypt the data encrypted on the primary node.
If the data decrypts successfully, Extensible Key Management using Luna EKM provider is operational.