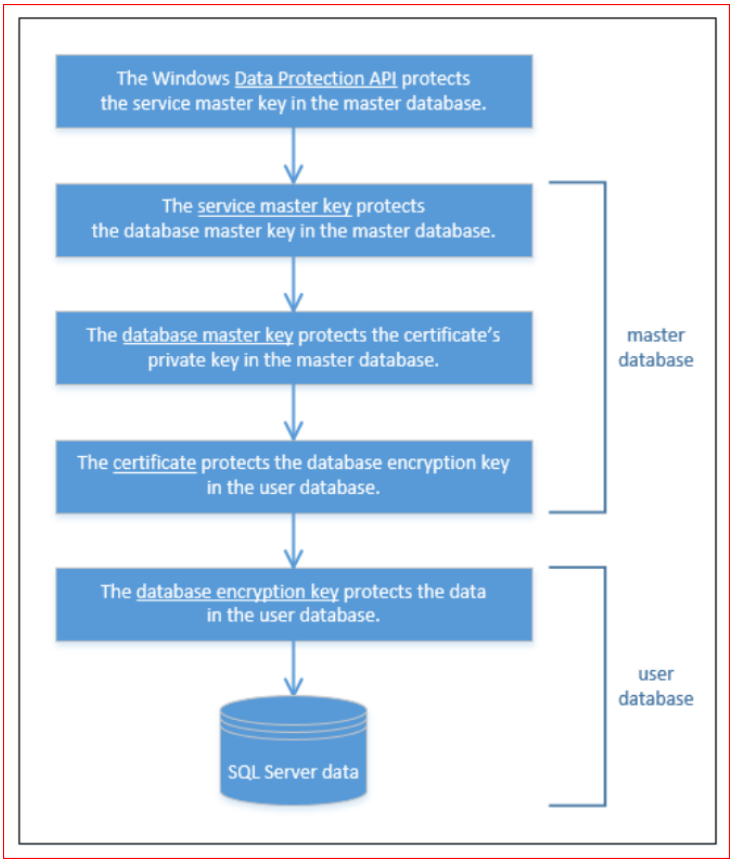
Enable TDE on Source DB - Restore TDE DB on Destination Server



****Please test below scripts in Dev/Test Environments thoroughly before working on Prod Servers.**

****I've tested below scripts in my LAB Machine and was working fine.**

At Source Server:

Step 1: Create Database Master Key, Backup Service Master Key, DB Master Key.

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION
BY PASSWORD='PraveenM@DBA$123';
GO
```

--Use this if Master key already exists and to add a new Master Key.

```
--ALTER MASTER KEY ADD ENCRYPTION BY PASSWORD ='PraveenM@DBA$123';
```

--Backup Service Master Key:

```
BACKUP SERVICE MASTER KEY
TO FILE = 'E:\MasterKey\SvcMasterKey.key'
ENCRYPTION BY PASSWORD = 'PraveenM@DBA$123'
```

--Backup DB Master Key:

```
BACKUP MASTER KEY
TO FILE = 'E:\MasterKey\DbMasterKey.key'
ENCRYPTION BY PASSWORD = 'PraveenM@DBA$123'
```

Step 2: Create a Certificate on Master DB to support TDE

```
USE master;
GO
CREATE CERTIFICATE TDE_Cert_New
WITH SUBJECT='Database_Encryption';
GO
```

Step-3: Backup Master DB Certificate & Private Key;

This step is not required to encrypt a database using TDE. But to make sure you can recover your encrypted data from a database backup, should your instance database become corrupted, or you want to move an encrypted database to another server, you should backup the certificate.

Run the following code:

```
USE master;
GO
BACKUP CERTIFICATE TDE_Cert_New
TO FILE = 'E:\MasterKey\TDE_Cert_New.cer'
WITH PRIVATE KEY(
 FILE = 'E:\MasterKey\TDE_Cert_New_PrivateKey.pvk',
 ENCRYPTION BY PASSWORD = 'PraveenM@DBA$123'
)
```

Note: Store the PASSWORD in a safe place.

Step 4: Create Database Encryption Key on required User DB.

```
USE Advworks
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE TDE_Cert_New;
```

Step 5: Enable TDE on Database

```
ALTER DATABASE Advworks SET ENCRYPTION ON;
```

At Destination Server:

Steps to Restore a TDE Database backup file of Source on Destination Server.

1) Create a new Master Key or Alter it using below if it already exists.

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD='PraveenM@DBA$123'; -- This can be from Source Server/New one.
--ALTER MASTER KEY ADD ENCRYPTION BY PASSWORD ='PraveenM@DBA$123'
```

2) Restore the Master DB Certificate of Source Server on Destination Server:

```
USE master;
GO
CREATE CERTIFICATE TDE_Cert_New
fROM  FILE = 'E:\MasterKey\TDE_Cert_New.cer'
WITH PRIVATE KEY(
 FILE = 'E:\MasterKey\TDE_Cert_New_PrivateKey.pvk',
 DECRYPTION  BY PASSWORD = 'PraveenM@DBA$123'
)
```

3) Finally Restore the TDE Enabled DB Backup File on Destination.

Reference Links:

https://www.sqlrx.com/sql-server-tde-encryption-and-query-performance/

https://www.sqlmatters.com/Articles/Setting%20up%20Transparent%20Data%20Encryption%20(TDE).aspx

https://pleasantsolutions.com/info/pleasant-password-server/b-server-configuration/4-changing-databases-for-pleasant-password-server/encrypt-your-database/sql-server-tde-encryption

https://www.red-gate.com/simple-talk/sql/sql-development/encrypting-sql-server-transparent-data-encryption-tde/