**TDE Encryption (instructions)**

**Overview:** Transparent Data Encryption (TDE) is a feature introduced in SQL Server 2008 and available in later versions for bulk encryption at the database file level (data file, log file and backup file) i.e. the entire database at rest.

Here are the 4 steps to encrypting a database:

1. Create a master key in master database.
2. Create a certificate protected by the master key that was created in step 1.
3. Create a database encryption key and protect it by the certificate.
4. Set the database to use encryption.

**Steps in details:**

1. **Create a master key by running this script:**

USE master;

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MyStrongPassword##!!';

GO

1. **Create a certificate by running this script:**

USE master;

CREATE CERTIFICATE HREWWDEVDB1218TDECert (or whatever you want to name it)

WITH SUBJECT = 'TDE Certificate'

GO

1. **Create a database encryption key and protect it by the certificate by running this script:**

USE EAPS;

CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES\_256

ENCRYPTION BY SERVER CERTIFICATE HREWWDEVDB1218TDECert

GO

1. **Enable encryption by running this script:**

ALTER DATABASE EAPS;

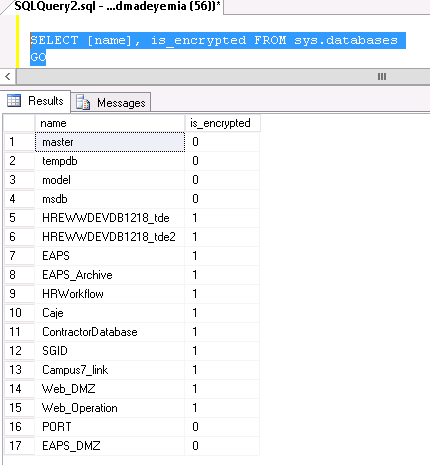
SET ENCRYPTION ON

GO

To verify that database is encrypted run this script:

SELECT [name], is\_encrypted FROM sys.databases

GO



If one needed to encrypt multiple databases, the same certificate that was created in the master database can be used to encrypt multiple databases on the same SQL Server instance you would simply run steps 3 and 4 above and change the database name (in step 3) to whatever database you needed encrypted. So instead of ‘use EAPS’ you would change that to ‘use EAPS\_DMZ’ in the example above as this database isn’t currently encrypted.

**To restore a database backup that is encrypted**:

1. Find the database name and corresponding certificate on the source server with this query:

select db\_name(dek.database\_id) AS ProtectedDB

, dek.create\_date

, c.name

, c.certificate\_id

, c.pvt\_key\_encryption\_type\_desc

, c.pvt\_key\_last\_backup\_date

, c.issuer\_name

, c.subject

, c.start\_date

, c.expiry\_date

from sys.dm\_database\_encryption\_keys dek

inner join master.sys.certificates c on dek.encryptor\_thumbprint = c.thumbprint

1. Create master key and add the certificate to the destination server:

--Create Master Key on Destination Server

USE master

GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'xxxxxxxxx'

GO

--Create cert and key on Destination from Source (the one we saved earlier)

CREATE CERTIFICATE TDECert2

FROM FILE = 'd:\tde\certificate\_TDE\_Test\_Certificate.cer'

WITH PRIVATE KEY (FILE = 'd:\tde\certificate\_TDE\_Test\_Key.pvk',

DECRYPTION BY PASSWORD = 'dontknowpassword')

1. Restore the database as usual.