

## Re: Encrypting Data using SQL Server 2005

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2007-11/msg00025.html>

---

- *From:* Kent Tegels <ktegels@xxxxxxxxxxxx>
  - *Date:* Wed, 7 Nov 2007 22:36:58 +0000 (UTC)
- 

Hello Greg,

GL> If you encrypt some data using a symmetric key with a password. It  
GL> appears that the database master key is not used at all to encrypt  
GL> the data. Is this true?

Strictly speaking, yes. But recall that the symmetric's key decryption device is stored encrypted by the Service Master (SMK) in its absence. So while the SMK isn't part the encryption vector per se, you aren't using going to be able to decrypt encrypted data without the correct SMK if you don't use a Database Master Key (DBMK).

GL> Also it appears you can backup the  
GL> database and move it to another server, and retrain the password for  
GL> the symmetric key from the old server. Meaning that after you  
GL> restore the database to a new server you can use the symmetric key  
GL> password from the old server to open the symmetric key in the  
GL> database on the new server and decrypt the data.

Yes, you wouldn't want to unrecoverable data, but you will still need to regenerate off that instance's SMK.

GL> My basic question if you create a symmetric key with a password, and  
GL> encrypt data with that symmetric key, then is there any reason you  
GL> would need to create a master key for the database?

Consider the following example. Although both DBs have the same keys, they really don't because the keys have different GUIDs. And if you look at the encrypted data carefully enough, its pretty obvious that the key guid is part of the encrypted data.

```
use master
go
create database enc1
create database enc2
go
use enc2
create table dbo.secrets(data varbinary(255))
go
use enc1
create symmetric key signingKey with algorithm = triple_des encryption by password = 'theKey'
open symmetric key signingkey decryption by password = 'theKey'
```

## Re: Encrypting Data using SQL Server 2005

```
create symmetric key enc_Key with algorithm = triple_des encryption by symmetric key signingKey
close symmetric key signingKey
go
open symmetric key signingkey decryption by password = 'theKey'
open symmetric key enc_key decryption by symmetric key signingKey
close symmetric key signingKey
select name,key_guid,algorithm_desc from sys.symmetric_keys
insert into enc2.dbo.secrets values (encryptByKey(key_guid('enc_key'),'beSureToDrinkYourOvaltine'))
select key_guid('enc_key'),data,cast(decryptByKey(data) as varchar(255)) from enc2.dbo.secrets
close symmetric key enc_key
go
use enc2
create symmetric key signingKey with algorithm = triple_des encryption by password = 'theKey'
open symmetric key signingkey decryption by password = 'theKey'
create symmetric key enc_Key with algorithm = triple_des encryption by symmetric key signingKey
close symmetric key signingKey
go
open symmetric key signingkey decryption by password = 'theKey'
open symmetric key enc_key decryption by symmetric key signingKey
close symmetric key signingKey
select name,key_guid,algorithm_desc from sys.symmetric_keys
select key_guid('enc_key'),data,cast(decryptByKey(data) as varchar(255)) from enc2.dbo.secrets
close symmetric key enc_key
go
```

.