

SQL Server Data Encryption 101

John Morehouse
Consultant

Denny Cherry & Associates Consulting



john@dcac.com



<http://linkedin.com/in/sqlrus>



@SqlRUs



<http://www.sqlrus.com>

Who Am I?

- Leader of the Louisville SQL Server/Power BI User Group
- Organizer/Speaker of SQL Saturday's & other conferences
- Heavily involved with SQL PASS
- Microsoft Data Platform MVP
- Friend of Redgate 2015 - 2018
- Idera ACE 2016
- SentryOne Product Advisory Council



Where Am I?



The vetted and certified experts at Denny Cherry and Associates Consulting assist companies with attaining IT goals such as HA, scalability, SQL Server virtualization, migration, and acceleration reliably while finding ways to save on costs. With clients ranging from Fortune 50 corporations to small businesses, their commitment to each is the same: to provide a deft, high-speed IT environment that leverages every aspect of their platform: from architecture, infrastructure, to network.

Visit DCAC at <http://www.dcac.co>

Quick Check

- How many:
 - DBA's
 - Developers
 - BI/DWH
 - Other
- Please make sure to fill out evaluations
- Ask questions!!!



If a data breach occurs....

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY



EVERY DAY

5,029,973

Records



EVERY HOUR

209,582

Records



EVERY MINUTE

3,493

Records



EVERY SECOND

58

Records

Encryption Options

- Let SQL Server do it
- Let the application do it
- Transparent Data Encryption (sorta, but not really)
 - Spectre/Meltdown
- Obfuscation/masking (not really encryption)



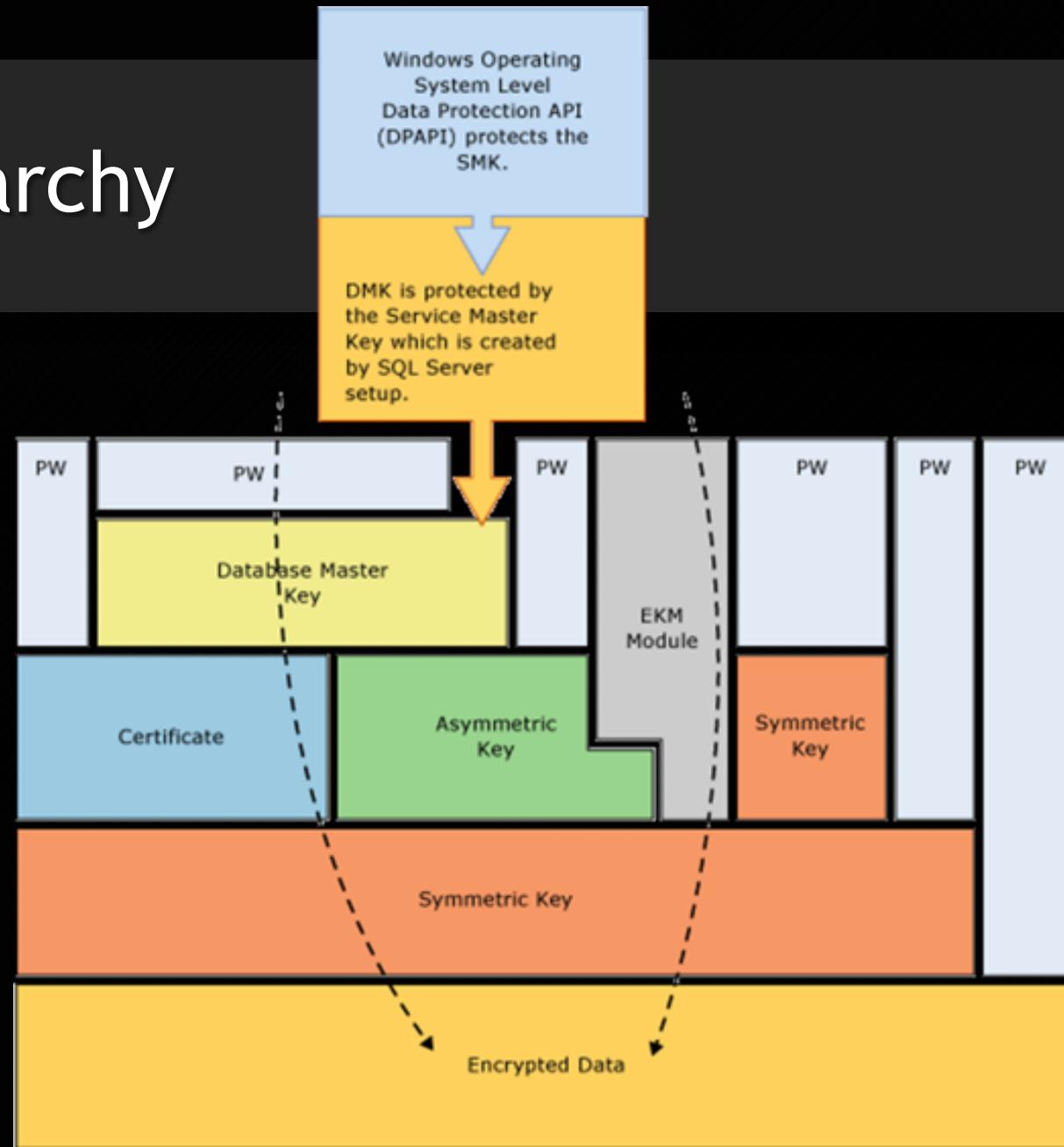
Terminology

- SMK
 - DMK
 - EKM
 - Asymmetric
 - Symmetric
 - Certificate



<https://www.shutterstock.com/image-photo/jargon-word>

Encryption Hierarchy



Symmetric		Other
ENCRYPTBYKEY	DECRYPTBYKEY	
ENCRYPTBYPASSPHRASE	DECRYPTBYPASSPHRASE	
KEY_ID	KEY_GUID	
DECRYPTBYAUTOASYMKEY	KEY_NAME	
SYMKEYPROPERTY		HASHBYTES
Asymmetric		DECRYPTBYKEYAUTOCERT
ENCRYPTBYASYMKEY	DECRYPTASYMKEY	
ENCRYPTBYCERT	DECRYPTBYCERT	
ASYMKEYPROPERTY	ASYMKEY_ID	

Native SQL Server Encryption

1

Generate
DMK

2

Choose
algorithm

3

Open the
key

4

Encrypt
the data

5

Close the
key

Process Flow

Demo

Trade offs

Causes CPU overhead

Cannot be compressed

Increased size of the data

Cannot be effectively indexed
HASHBYTES

Cannot exceed VARBINARY(8000)

Watch out for character lengths/data types

Possibly significant schema changes

Application changes if encryption is done within the application

Always Encrypted

- SQL Server 2016 or higher
- SQL Server has zero knowledge of keys
- Combines SQL Server & Application
- Transparent to application
- Gets the DBA out of the data
- Deterministic/Randomized Encryption



<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017>

However.....

Always Encrypted Gotchas

Different collation on encrypted columns (BIN2)

No Default constraints

No partition columns

Columns reference by computed columns

No transactional/merge replication

Searching can be difficult

What about reports?

Definitely requires appdev time/resources

3rd Party Head Fake

- 3rd Party CRM
- Data encrypted where appropriate
- Call to a CLR Function handled the encryption
- Password stored in another database/table

IN CLEAR TEXT

The screenshot shows a SQL Server Management Studio window with three tabs at the top: 'SQLQuery9.sql - WI...6\jmorehouse (56)*' (selected), 'SQLQuery8.sql - WI...6\jmorehouse (55)*', and 'SQLQuery7.sql -'. The main pane displays the following T-SQL script:

```
use Scratch
GO

CREATE TABLE dbo.NoNo ([password] nvarchar(100))
GO
INSERT dbo.NoNo ([password]) VALUES ('I cannot believe it is really here!!')
GO
SELECT [password] FROM dbo.NoNo
```

The 'Results' tab is selected, showing the output of the SELECT statement:

	password
1	I cannot believe it is really here!!

3rd Party Head Fake

3rd Party Head Fake

The screenshot shows a SQL Server Management Studio window with two tabs open:

- Query9.sql - WI...6\jmorehouse (56)***: Contains T-SQL code to create a symmetric key and select from sys.symmetric_keys and sys.certificates.
- SQLQuery8.sql - WI...6\jmorehouse (55)***: Contains T-SQL code to select from sys.symmetric_keys and sys.certificates.

The results pane displays the output of the second query, showing two rows of data:

name	principal_id	symmetric_key_id	key_length	key_algorithm
##MS_DatabaseMasterKey##	1	101	256	A3
DBEncryption	1	256	256	A3

Below this, another table is partially visible:

name	certificate_id	principal_id	pvt_key_encryption_type	pvt_key_encryption_type
Encryption_Test	256	1	MK	ENCRYPTED_BY_MA

```
--update the altered table with the encrypted value using the symmetric key  
UPDATE dbo.NoNo  
SET Encrypted = ENCRYPTBYKEY(KEY_GUID('DBEncryption'),[password]) --clear_text  
GO  
SELECT * from dbo.NoNo
```

100 % < |

Results Messages

	password	Encrypted
1	I cannot believe it is really here!!	0x00813ED39F0C6F4F9425742CA7CF64BB0100000064B11E...

3rd Party Head Fake

```
--rename the table  
EXEC sp_rename 'NoNo', 'NoNo_Maybe'  
GO  
-- create the new view  
CREATE VIEW dbo.NoNo  
AS  
SELECT CONVERT(NVARCHAR(100),DECRYPTBYKEYAUTOCERT(CERT_ID('Encryption_Test'),NULL,encrypted)) AS 'NowYouSeeMe'  
FROM dbo.NoNo_Maybe  
GO  
SELECT * FROM dbo.NoNo  
SELECT * FROM dbo.NoNo_Maybe
```

100 % < III

Results Messages

	NowYouSeeMe
1	I cannot believe it is really here!!

	password	Encrypted
1	I cannot believe it is really here!!	0x00813ED39F0C6F4F9425742CA7CF64BB0100000064B11E...

3rd Party Head Fake

Questions



- <https://docs.microsoft.com/en-us/sql/t-sql/functions/cryptographic-functions-transact-sql?view=sql-server-2017> (starting with 2008)
- <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-2017>
- <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine?view=sql-server-2017>
- <https://docs.microsoft.com/en-us/sql/t-sql/statements/create-certificate-transact-sql?view=sql-server-2017>
- <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/create-identical-symmetric-keys-on-two-servers?view=sql-server-2017>

Resources

THANK YOU!!!!



john@dcac.com



@SqlRUs



<http://linkedin.com/in/sqlrus>



<http://www.sqlrus.com>