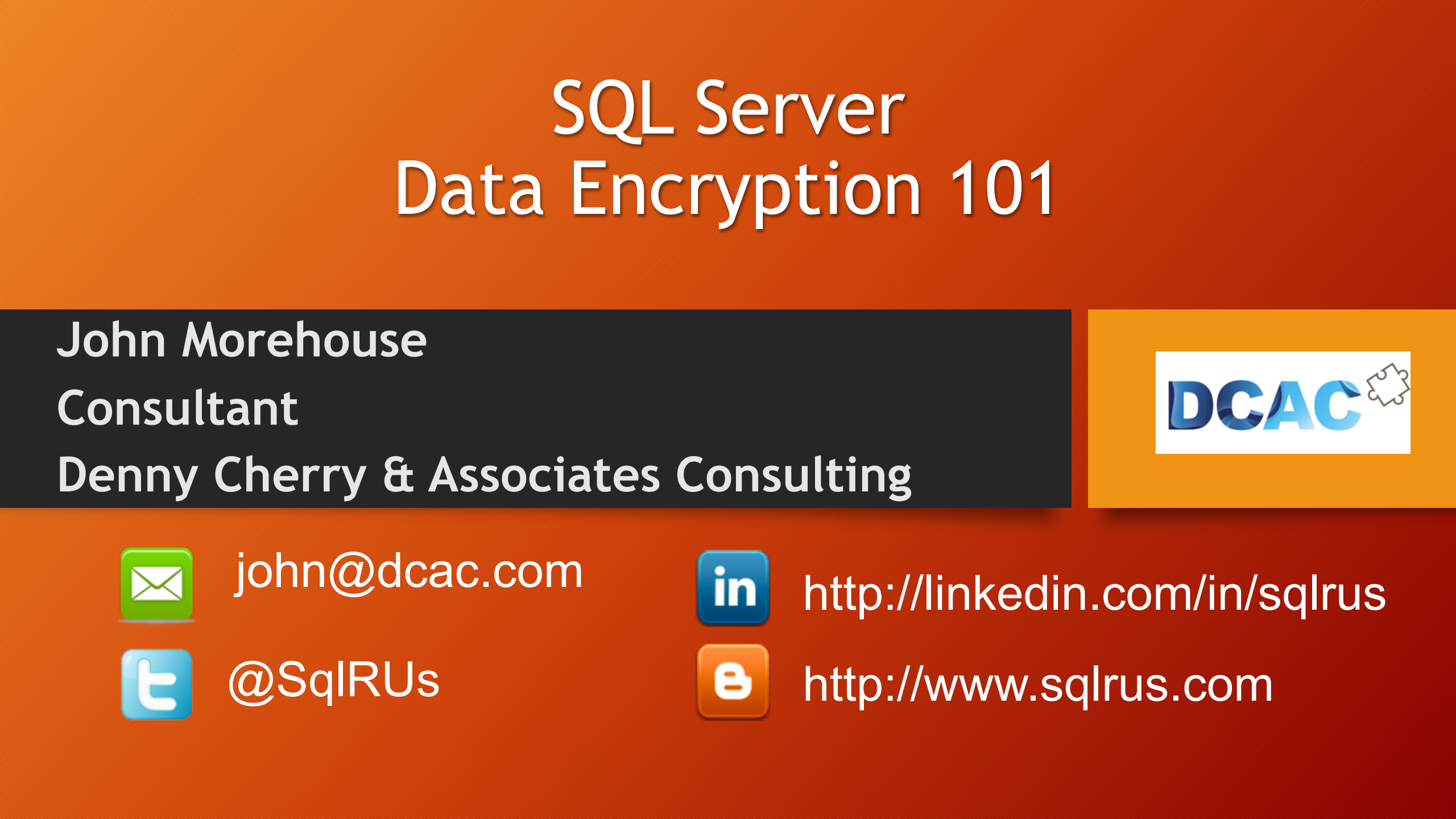
SQL Server Data Encryption 101

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….

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)

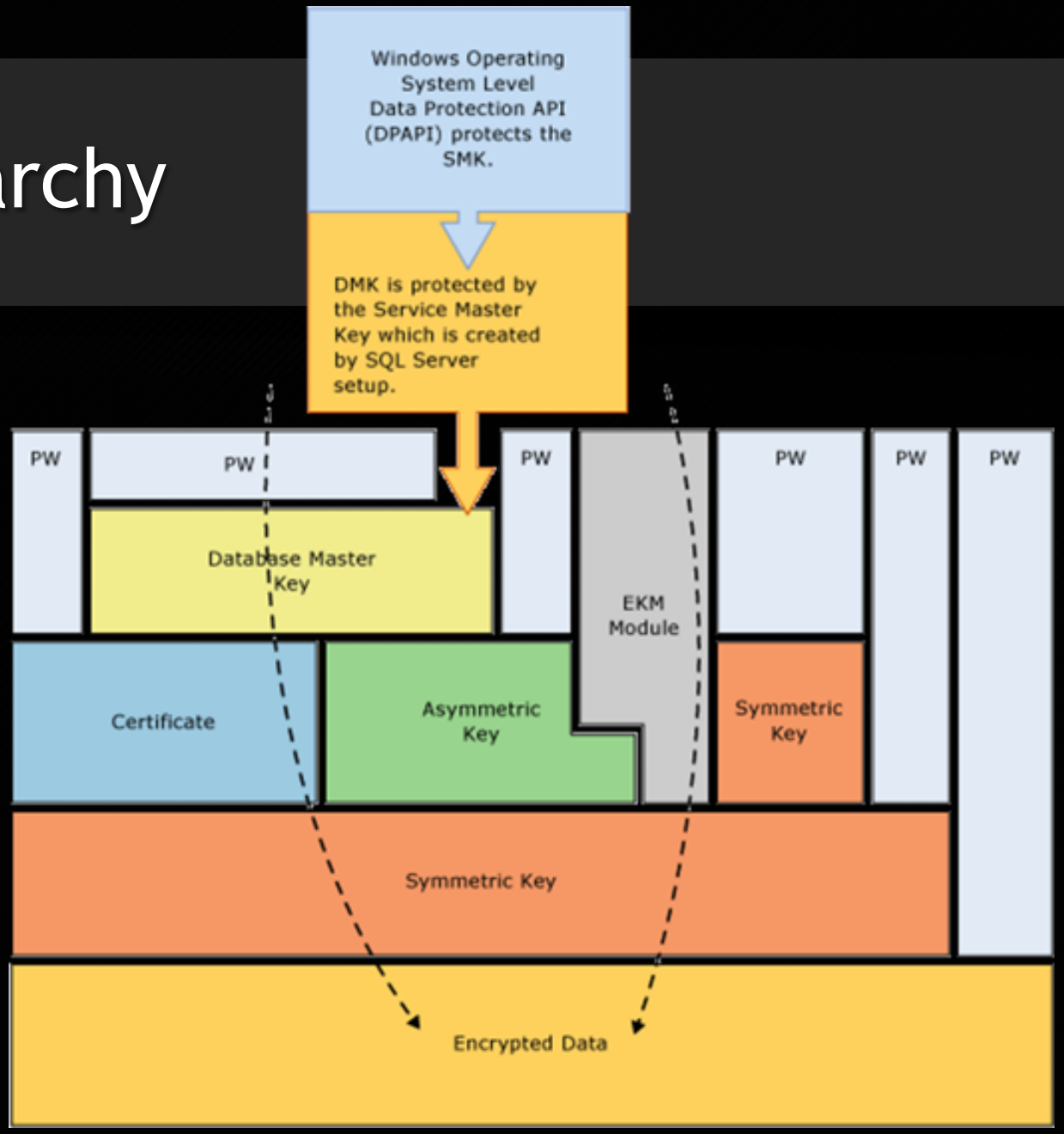
https://pixabay.com/en/security-secure-technology-safety-2168234/

Terminology

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

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

Encryption Hierarchy



Symmetric	
ENCRYPTBYKEY	DECRYPTBYKEY
ENCRYPTBYPASSPHRASE	DECRYPTBYPASSPHRASE
KEY_ID	KEY_GUID
DECRYPTBYAUTOASYMKEY	KEY_NAME
SYMKEYPROPERTY	

Asymmetric	
ENCRYPTBYASYMKEY	DECRYPTASYMKEY
ENCRYPTBYCERT	DECRYPTBYCERT
ASYMKEYPROPERTY	ASYMKEY_ID

Other
HASHBYTES
DECRYPTBYKEYAUTOCERT

Native SQL Server Encryption

Process Flow

1. Generate DMK
2. Choose algorithm
3. Open the key
4. Encrypt the data
5. Close the key

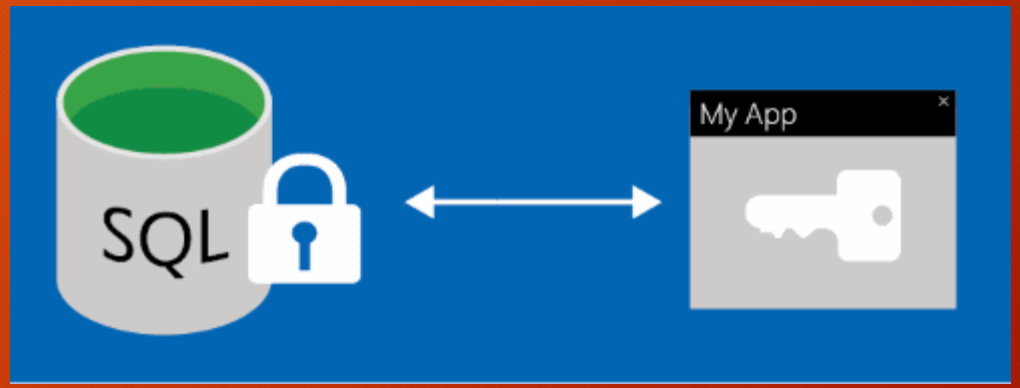

Demo

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…..

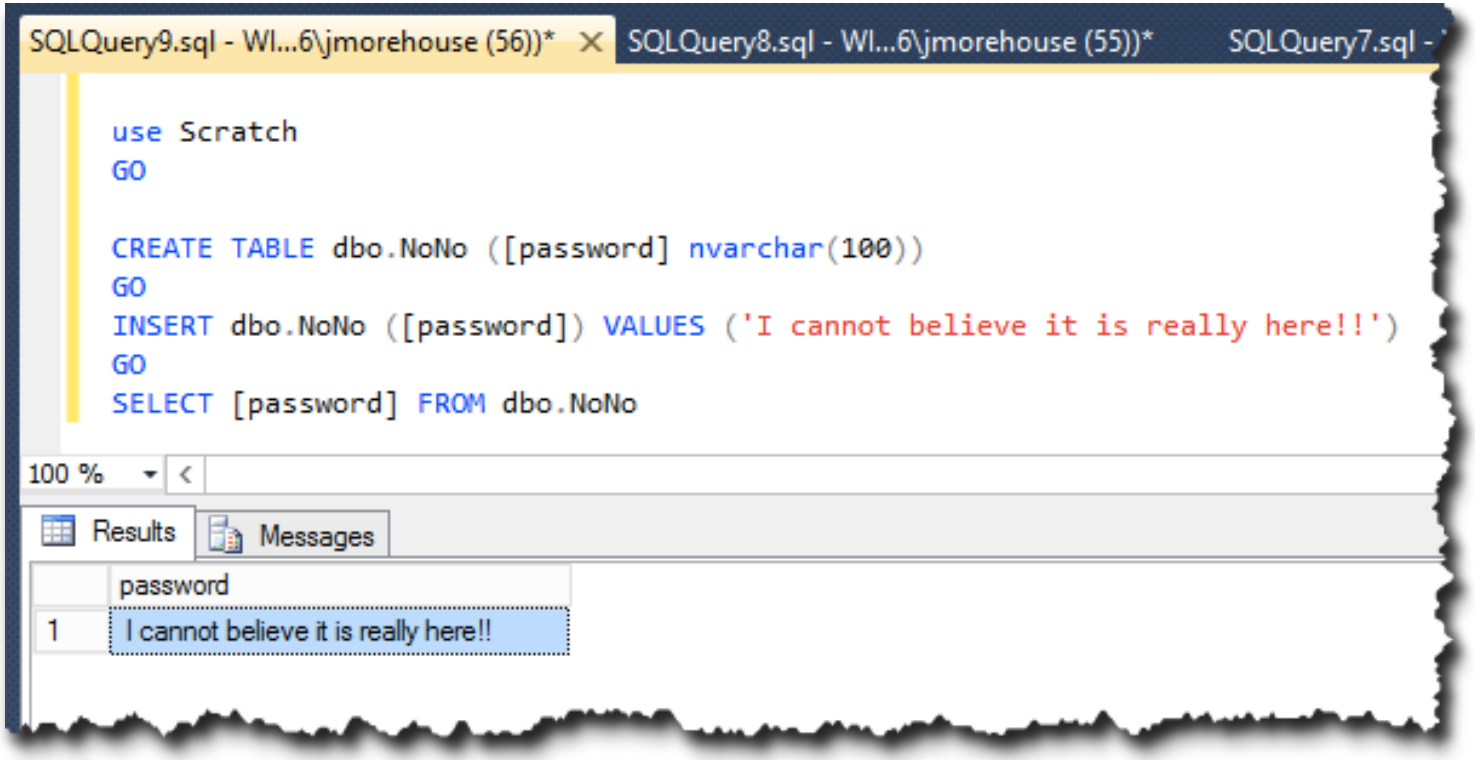
Always Encrypted Gotchas

- 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

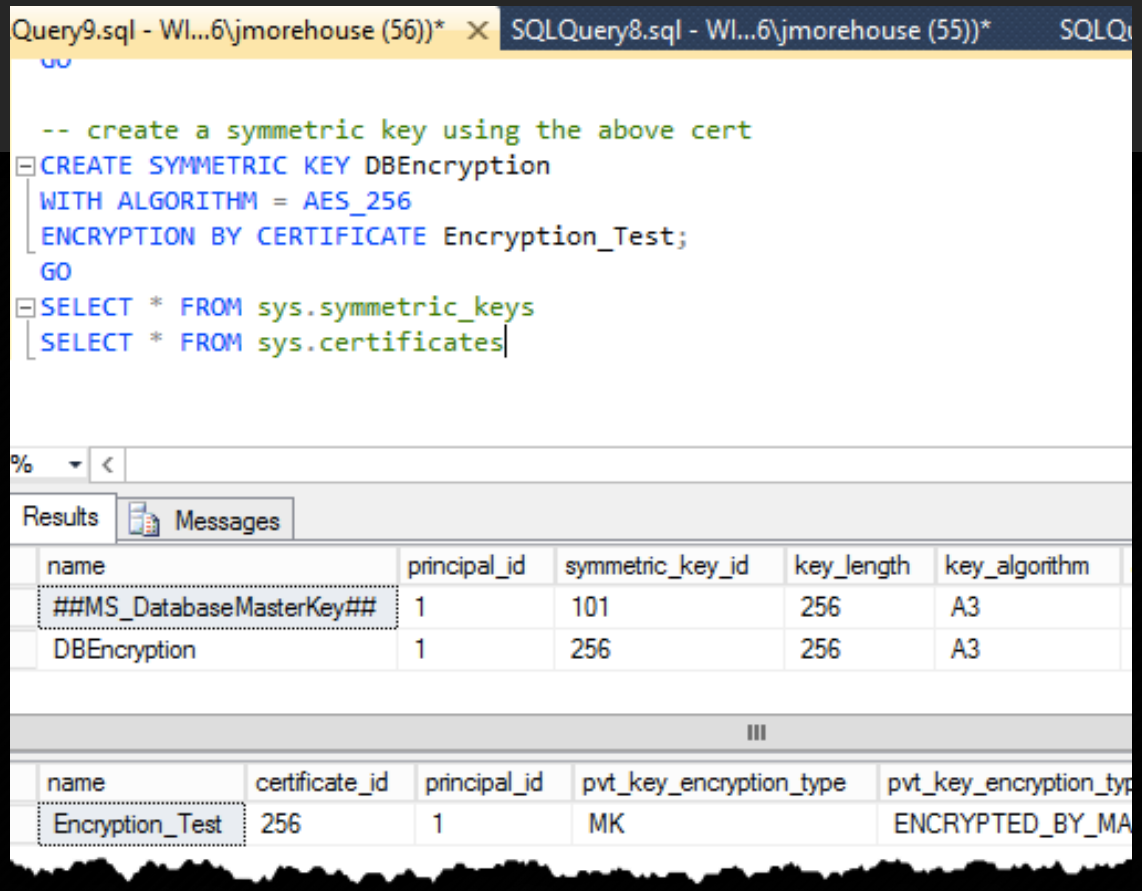
3rd Party Head Fake

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

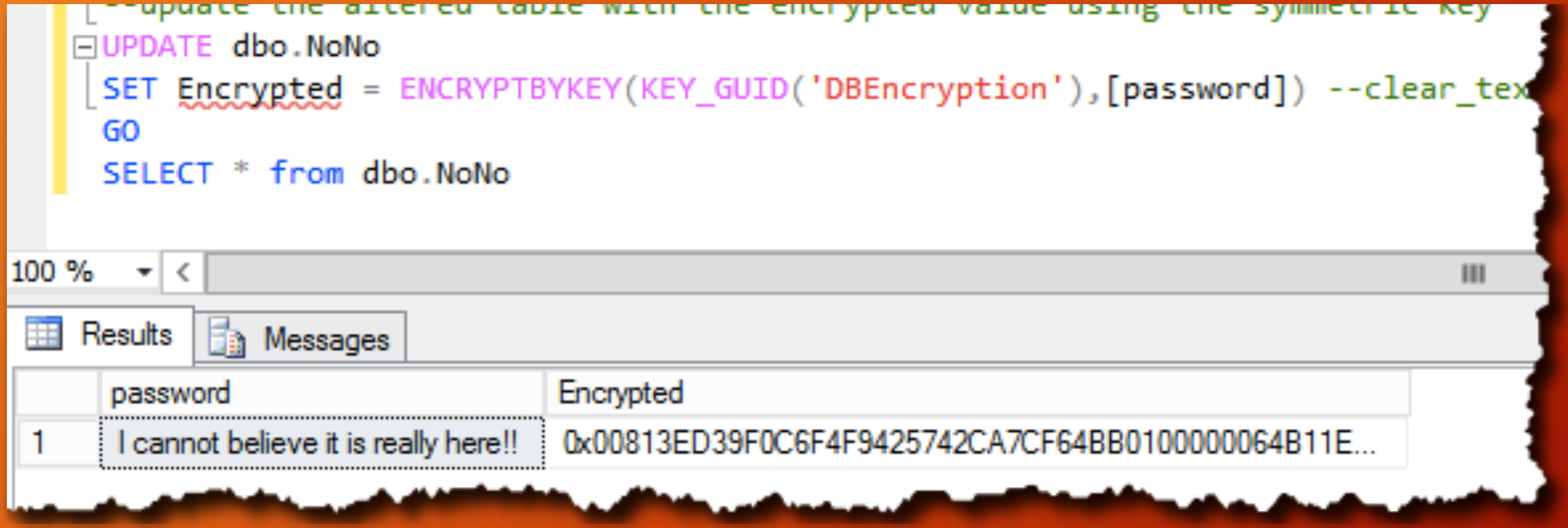
IN CLEAR TEXT



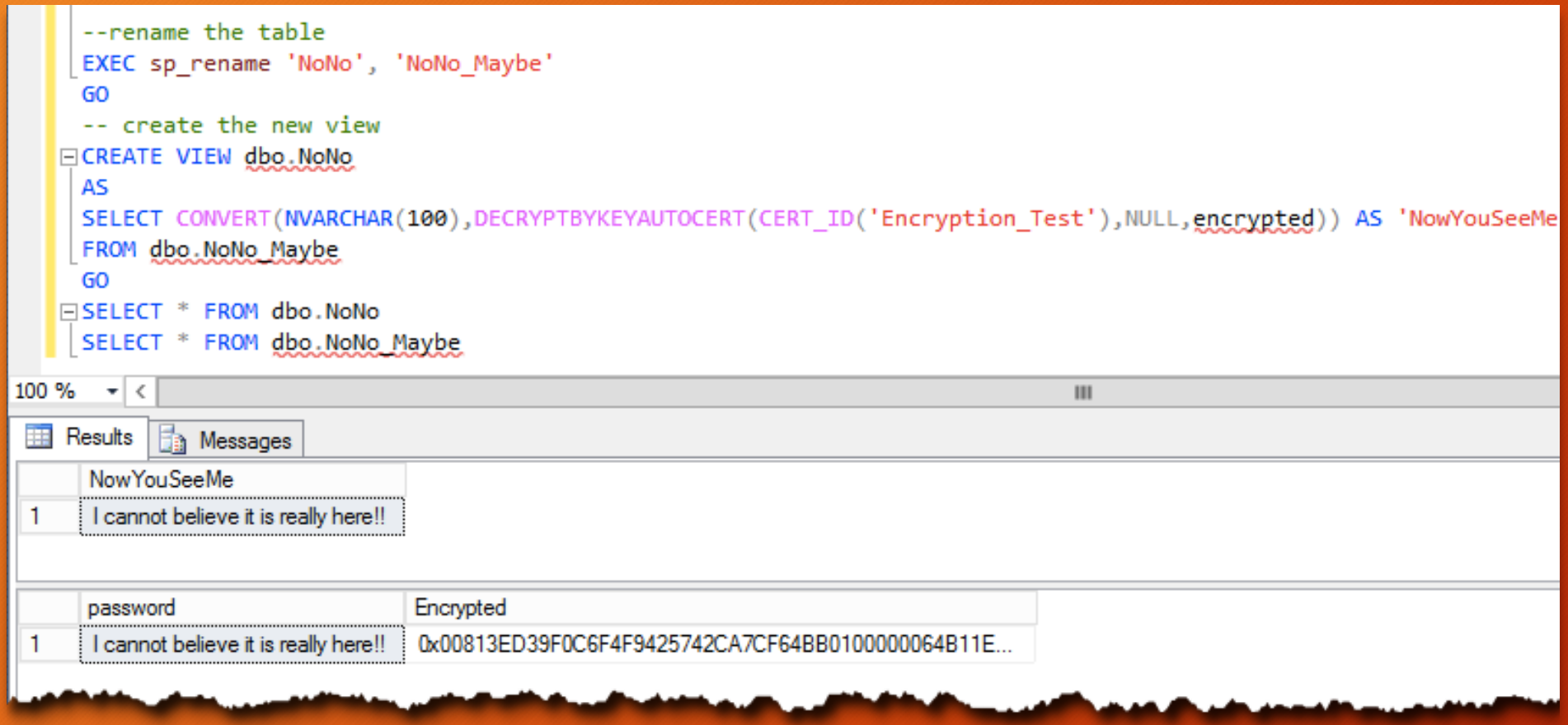
3rd Party Head Fake



3rd Party Head Fake



3rd Party Head Fake



3rd Party Head Fake

Questions

Resources

- 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

THANK YOU!!!!

john@dcac.com


@SqlRUs


http://linkedin.com/in/sqlrus


http://www.sqlrus.com