

Always Encrypted

Beginners 101 Guide to Always Encrypted

Monica Rathbun, Consultant

Denny Cherry and Associates
Consulting



SQLEspresso



Monica Rathbun

Consultant

Denny Cherry & Associates Consulting



Your Barista For SQL Knowledge!



/sqlsespresso



@SQLEspresso



SQLEspresso

SQLEspresso.com



Presentation Rules

Always Ask Questions

Interrupt me

This is a two-way conversation
let's learn from each other's
experiences

AGENDA



01

TERMINOLOGY

02

WHAT IT IS

03

GOTCHAS

04

KEYS

05

SECURE
ENCLAVES

06

USING IT

IF TIME ALLOWS

DEMOS

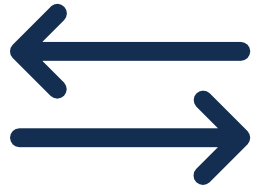


THE BASIC TERMINOLOGY

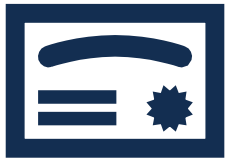
WHAT IS ENCRYPTION?



ENCRYPTION TERMINOLOGY



Encrypt & Decrypt



Certificates



Keys



Vaults

TYPES OF ENCRYPTION

Type	Usage	Things to Note
Transparent Data Encryption (TDE)	Database Level	Data at Rest, Decrypted while in motion from Memory to Storage processor.
Column Level Encryption	Column Level	DBA Can Get to Data, SQL Knows the Keys
Dynamic Data Masking	Column Level	Not Really Encryption
Always Encrypted	Column Level	Encrypted Everywhere For Everyone

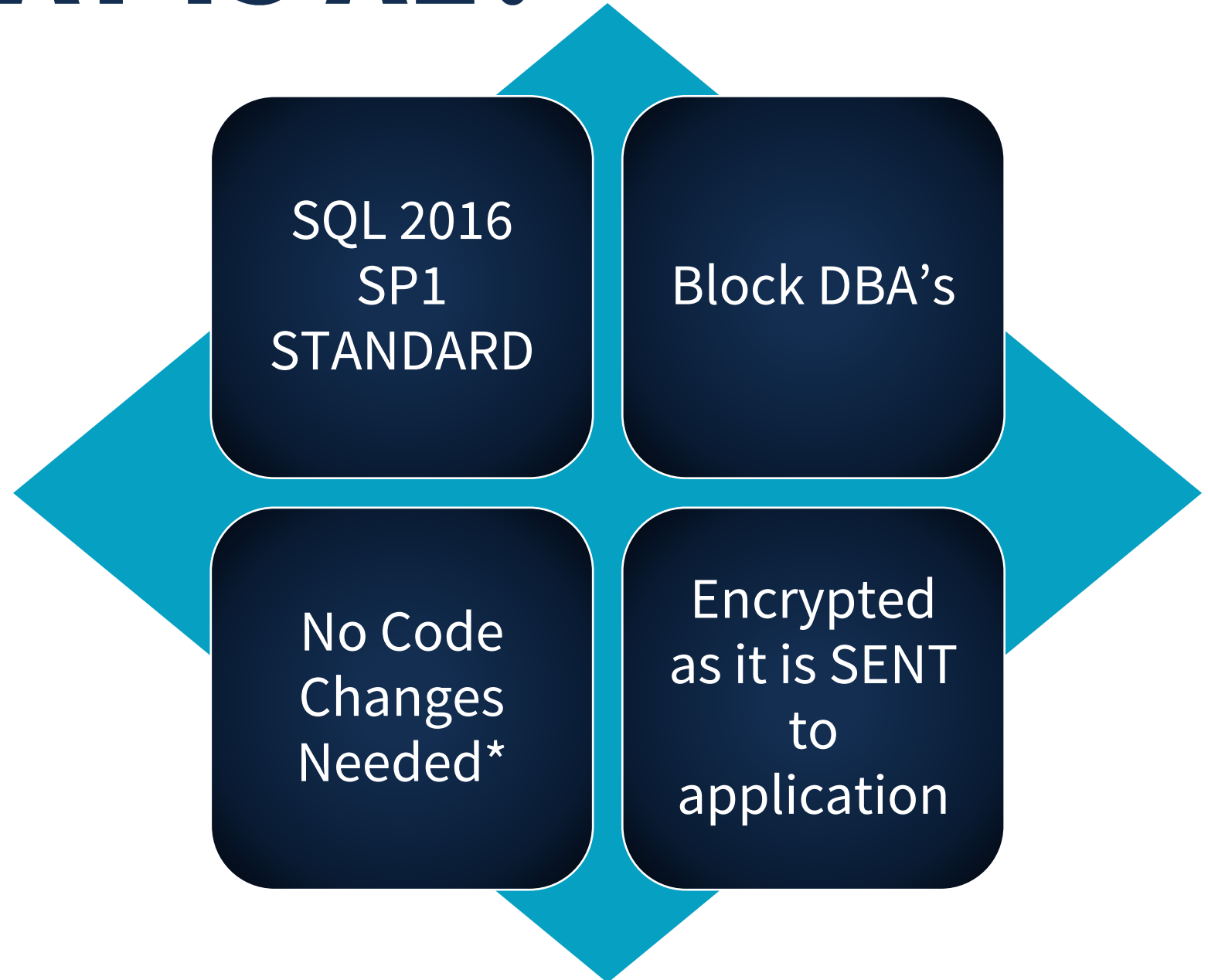


WHAT & HOW IT WORKS

WHAT IS AE?



**ALWAYS
ENCRYPTED**



TWO TYPES OF AE



**ALWAYS
ENCRYPTED**

Deterministic

ABCACBACB

WHERE clauses,
GROUP BY and
JOINS

Indexes

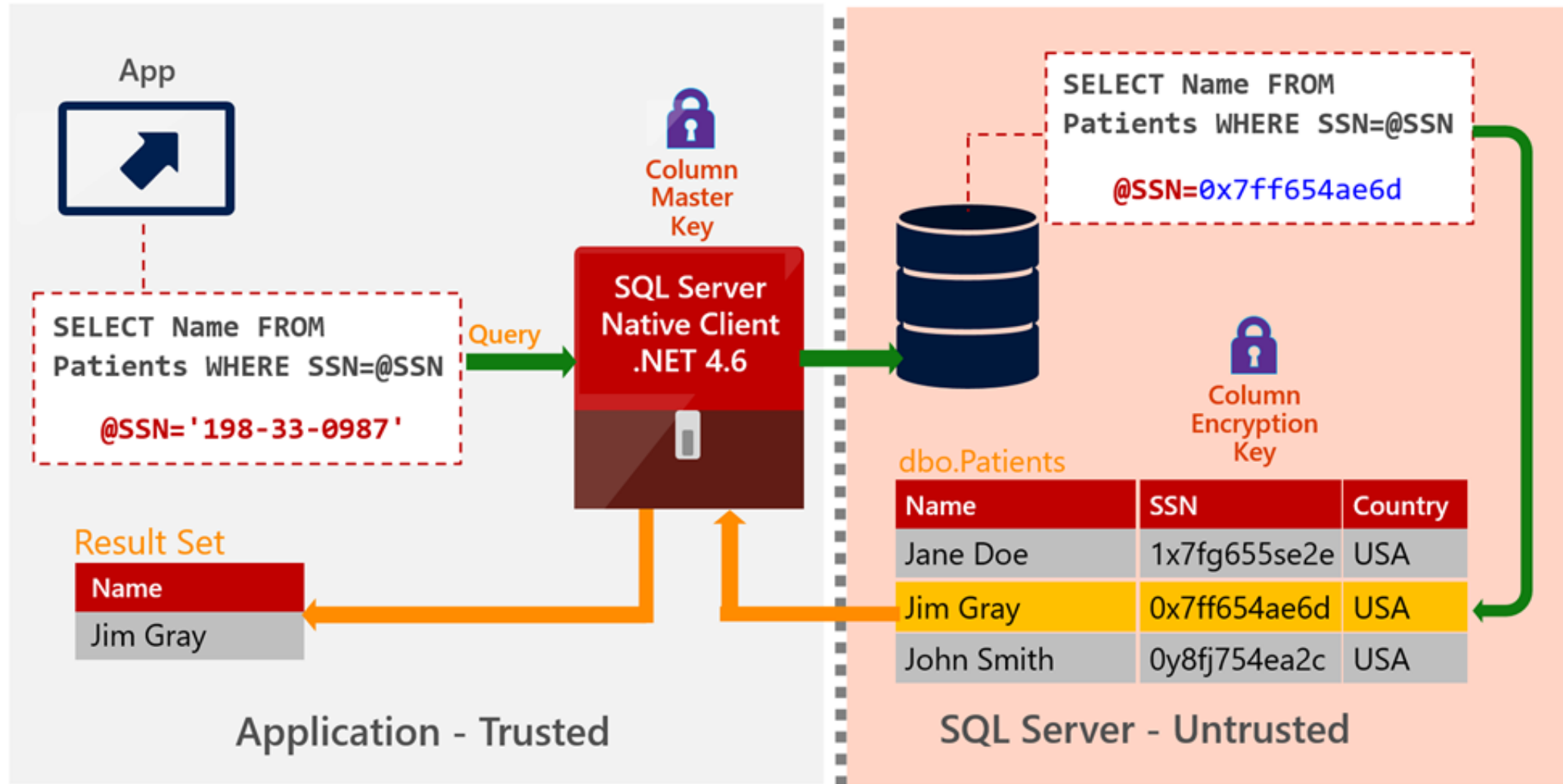
Randomize

ABCACBACB,
BBBCCAA, or
CCCAAABBB

More Secure

Non-Searchable

HOW IT WORKS





AE

GOTCHAS

AE GOTCHAS



Distributed
Queries (linked
servers)

No Default Or
Check
Constraints

No Partition
Columns

Columns
Reference By
Computed
Columns

No
Transactional/
Merge
Replication

Aggregations

Columns with
the IDENTITY
property

No Triggers



KEYS

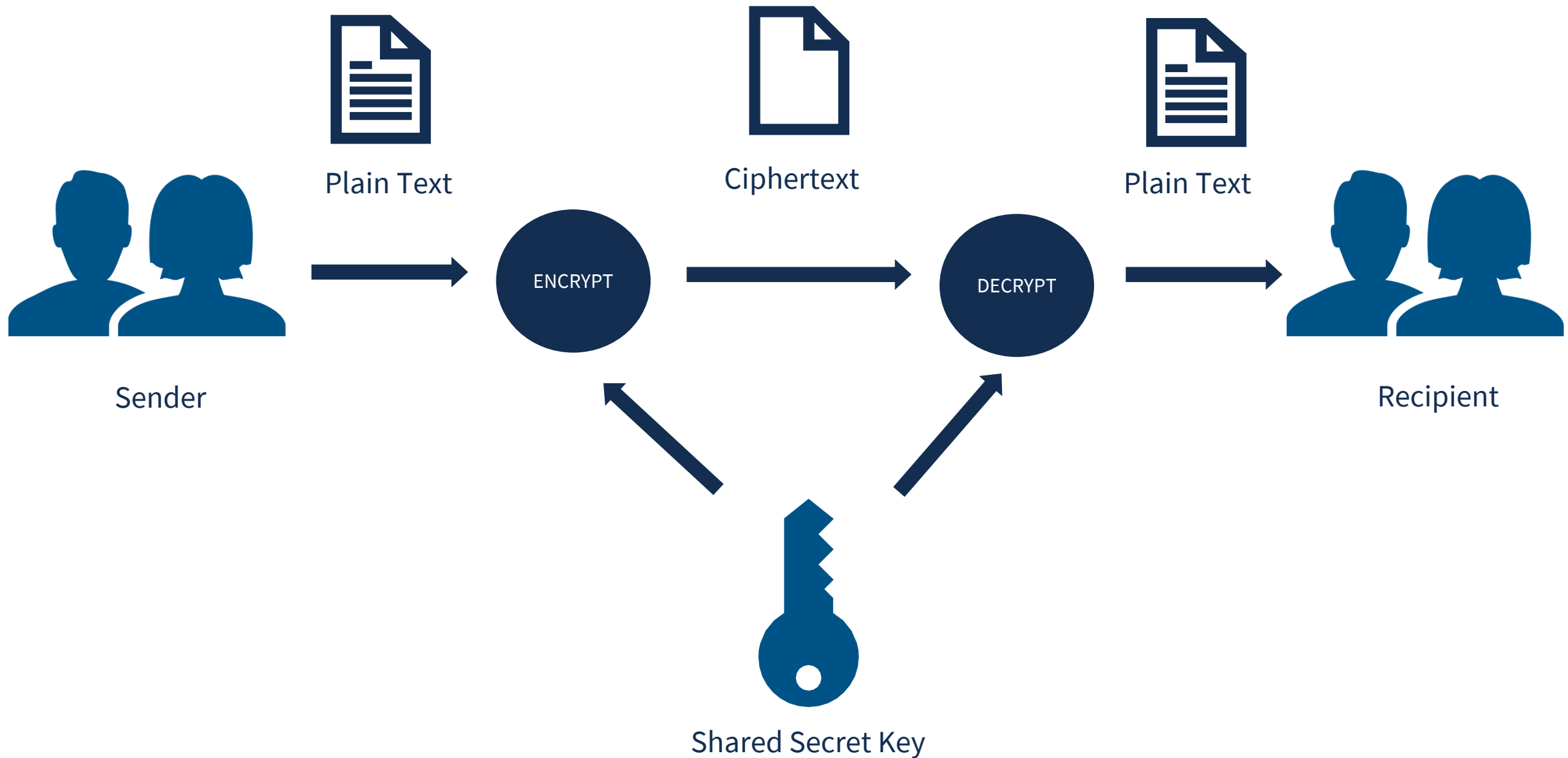
ALWAYS ENCRYPTED KEYS

Column Encryption Key (CEK)

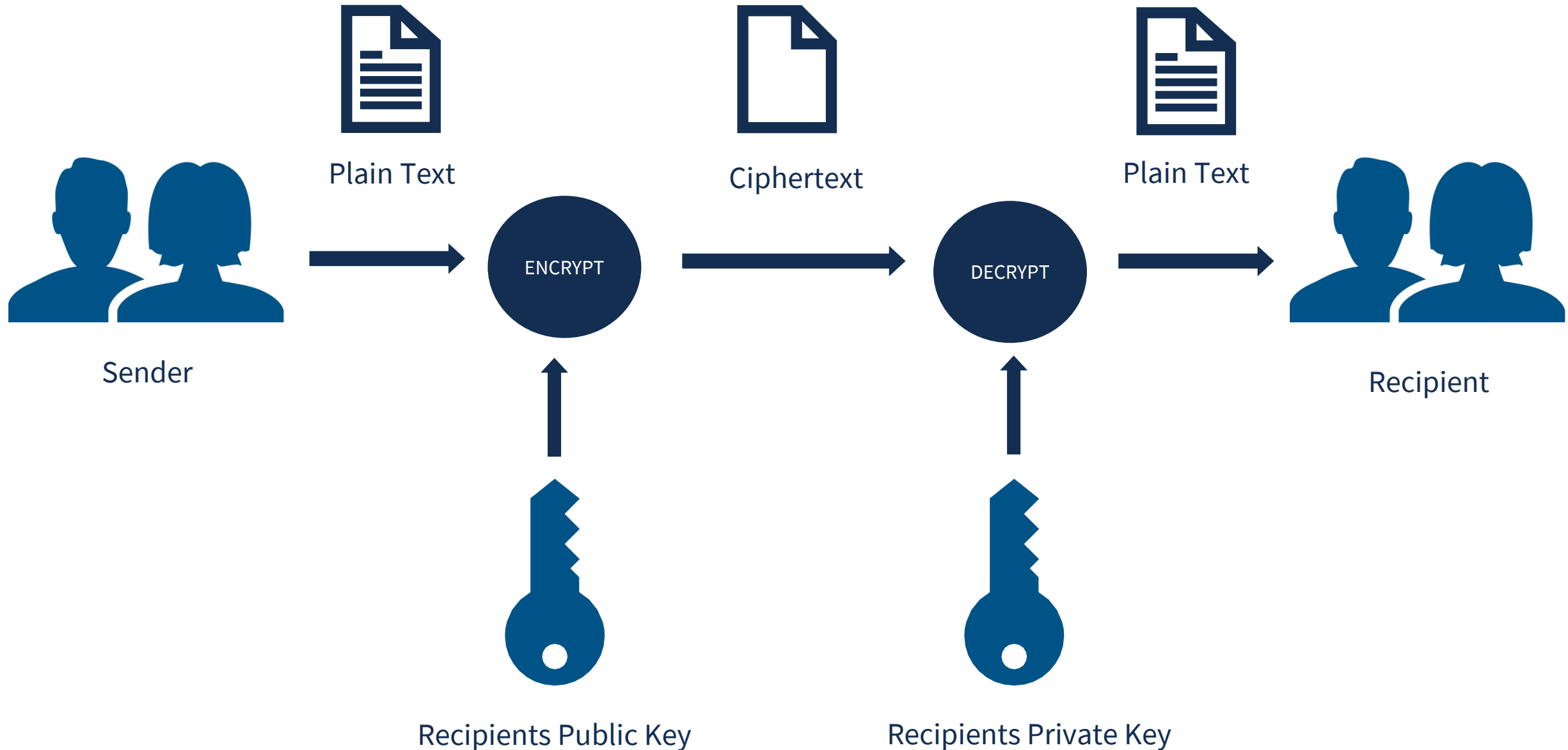
Column Master Keys (CMK)



SYMMETRIC KEY ENCRYPTION



ASYMMETRIC KEY ENCRYPTION



COLUMN ENCRYPTION KEY



Content Encryption Keys



1 or More Columns



Encrypted by Column Master Key



Column Encryption Key Metadata Stored in Database

COLUMN MASTER KEY



Protects CEK



Must Be Stored in Trusted Key Store



**Database only Contains Metadata of CMK
Keystore and Location Only**



`Sys.column_master_keys`

STORING KEYS



Windows Certificate Store



**Local to Server
Needs Deployed to
Each Server**

AZURE Key Vault



**AZURE Subscription
Reliable Internet**

WINDOWS CERTIFICATE STORE



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

Console Root

- Certificates - Current User
 - Personal
 - Certificates
 - Trusted Root Certification Authorities
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Active Directory User Object
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certification Authorities

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
Always Encrypted Auto Certificate1	Always Encrypted Auto Certificate1	11/29/2018	IP security IKE inter...	<None>
Always Encrypted Auto Certificate2	Always Encrypted Auto Certificate2	11/29/2018	IP security IKE inter...	<None>
monica@dcac.co	Communications Server	11/29/2017	Client Authentication	<None>
S-1-12-1-3380741540-1216562619-374886009...	S-1-12-1-3380741540-1216562619...	9/15/2047	Smart Card Logon	<None>

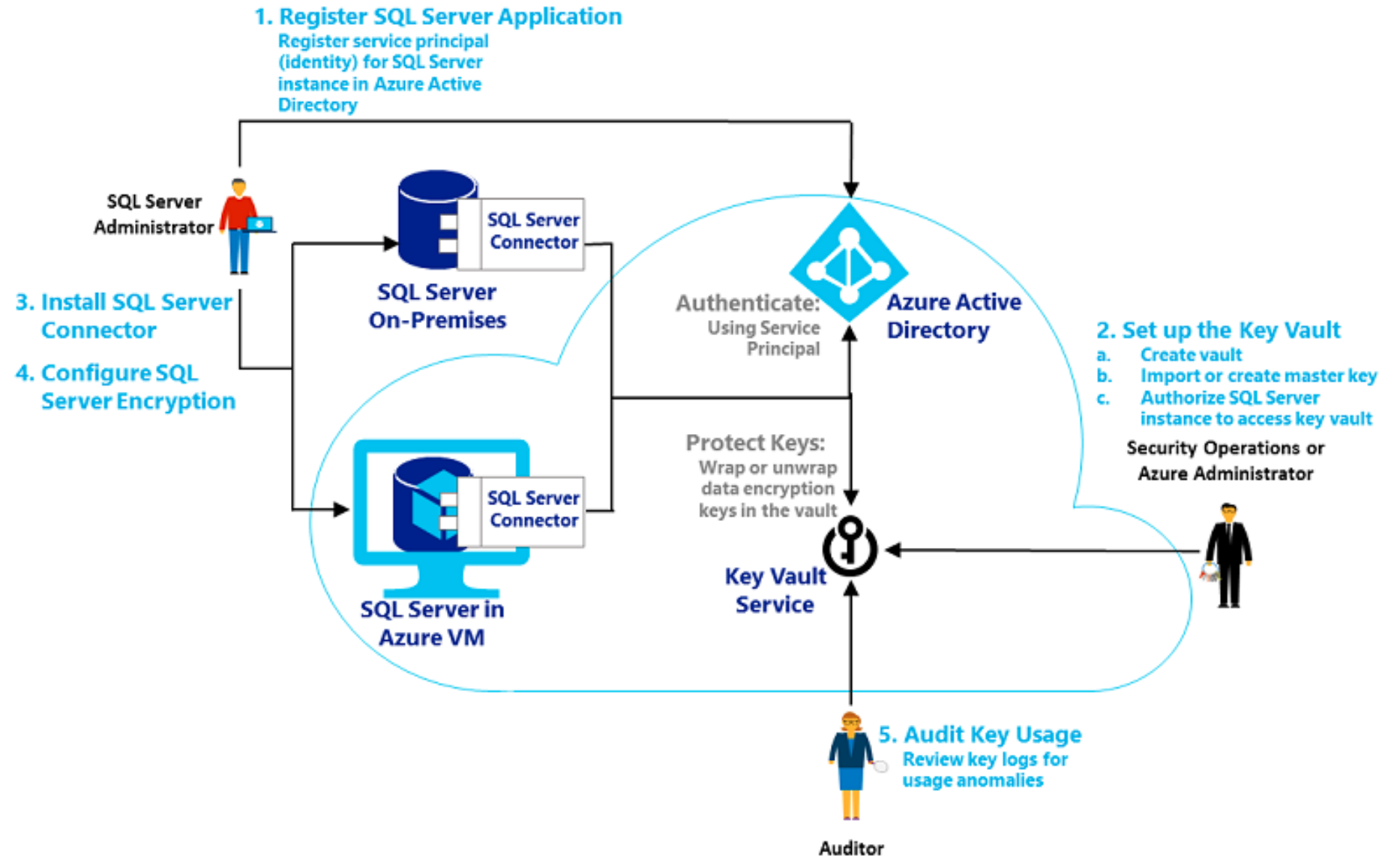
Two certificate locations: *local machine* or *current user*

Key store exists on each machine hosting your application

AZURE KEY VAULT



ALWAYS
ENCRYPTED



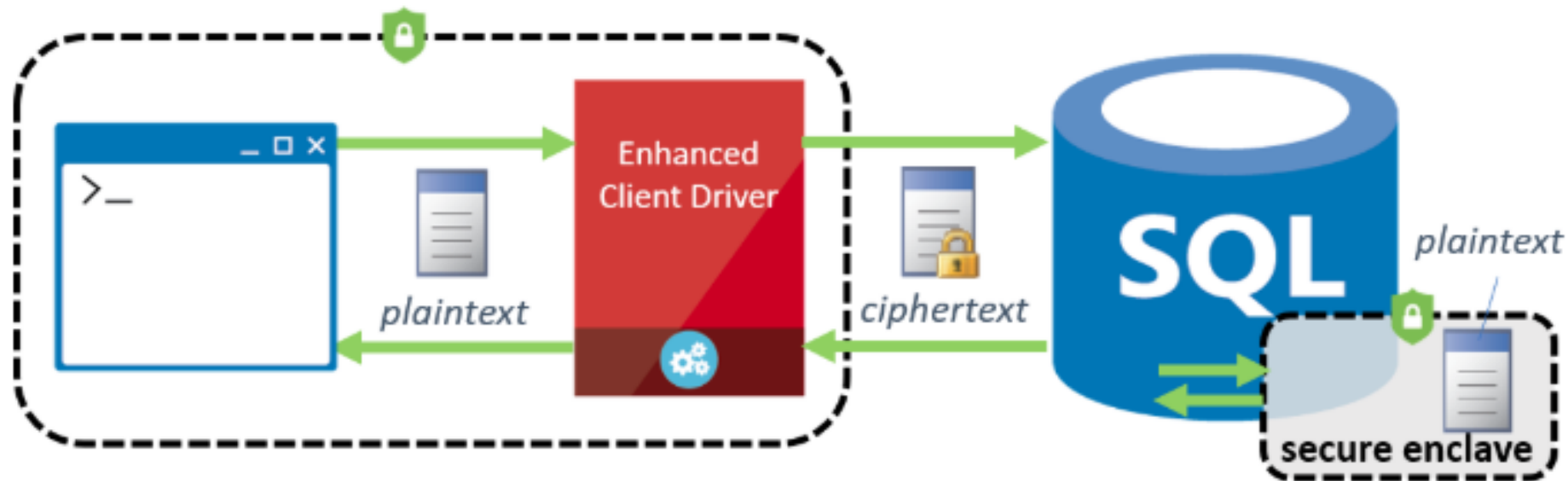


SECURE ENCLAVES

WHAT IS AN ENCLAVE?



An enclave is a protected region of memory that acts as a trusted execution environment.





**ALWAYS
ENCRYPTED**

RICH COMPUTATIONS

Pattern Matching

Range Comparisons

Sorting

DBCC traceon (127,-1)

IN-PLACE ENCRYPTIONS

In-Place Encryptions

Initial Data Encryption

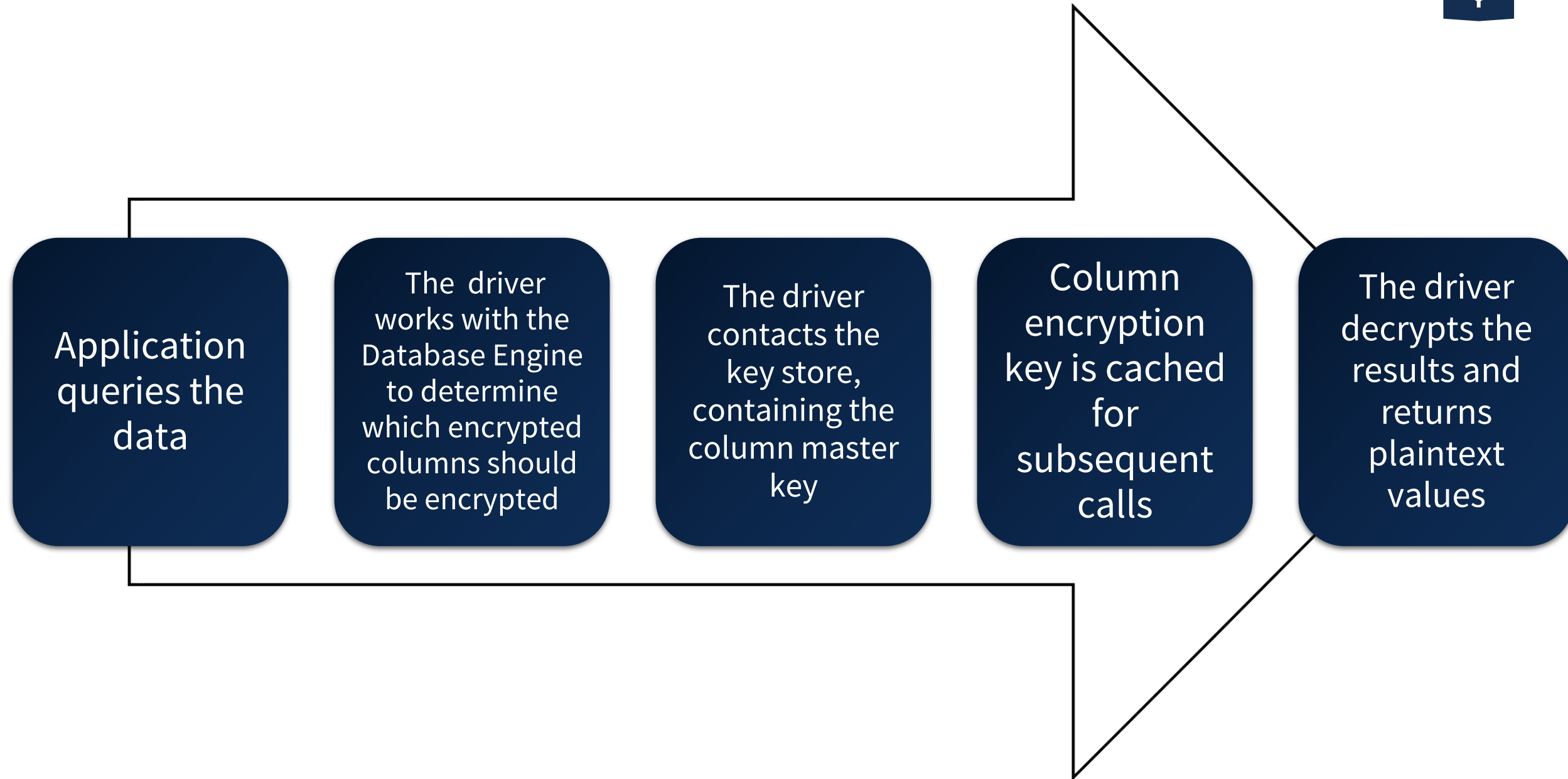
Rotating a Column Encryption Key

Changing a Data Type of an
Encrypted Column



**ALWAYS
ENCRYPTED**

HOW IT WORKS

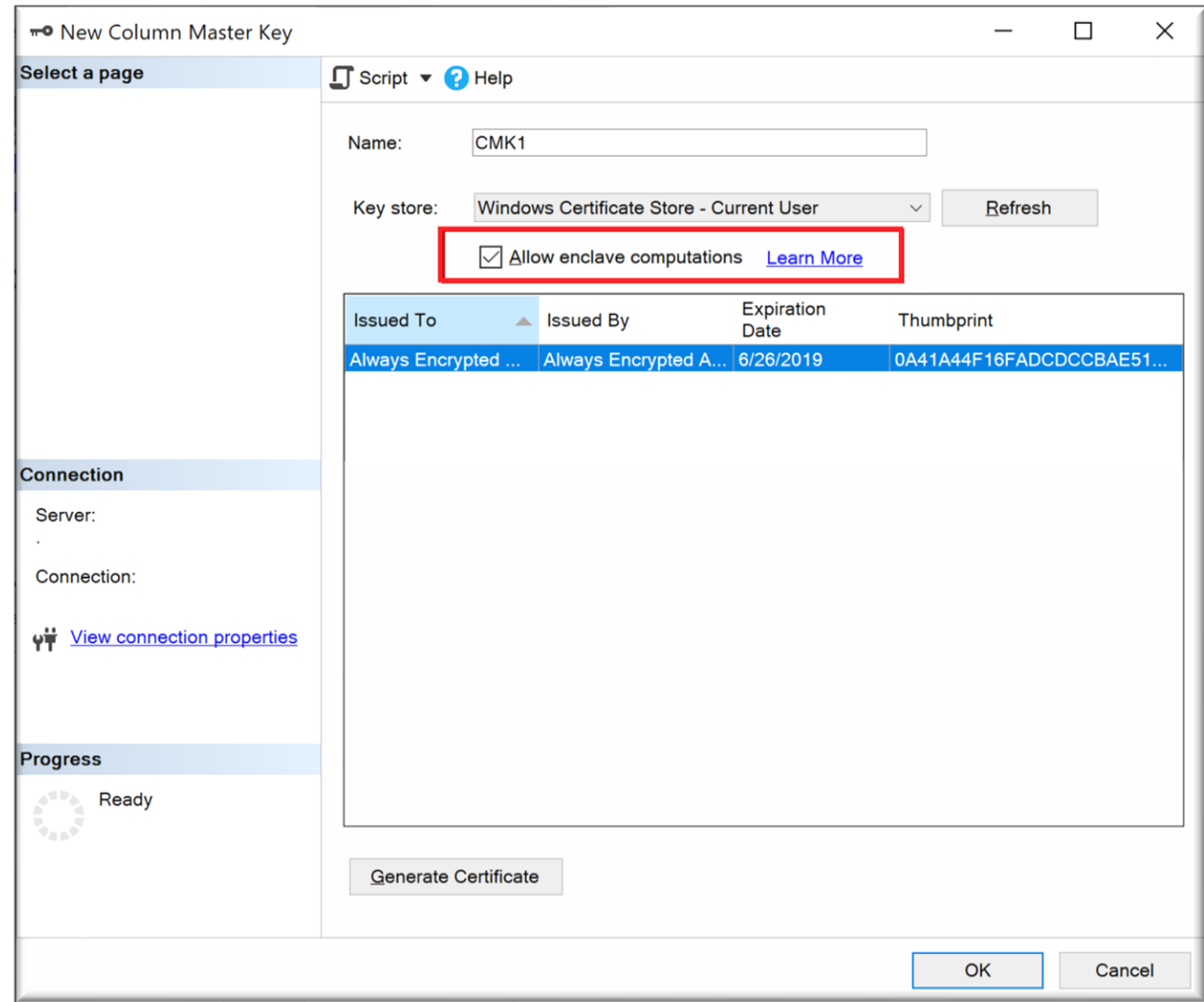
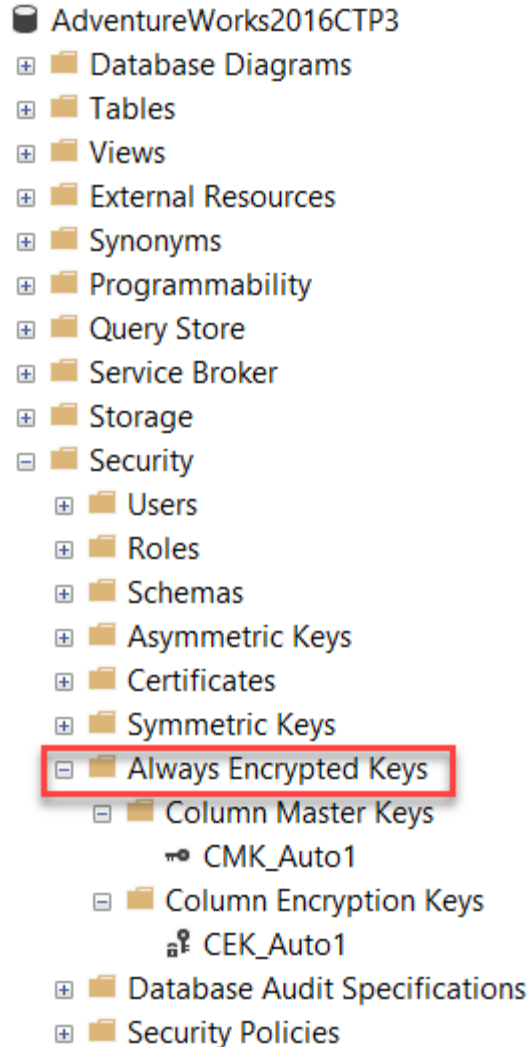




USING
ALWAYS
ENCRYPTED

SQL SERVER 2019 ENCLAVES

SSMS 18.0 or HIGHER

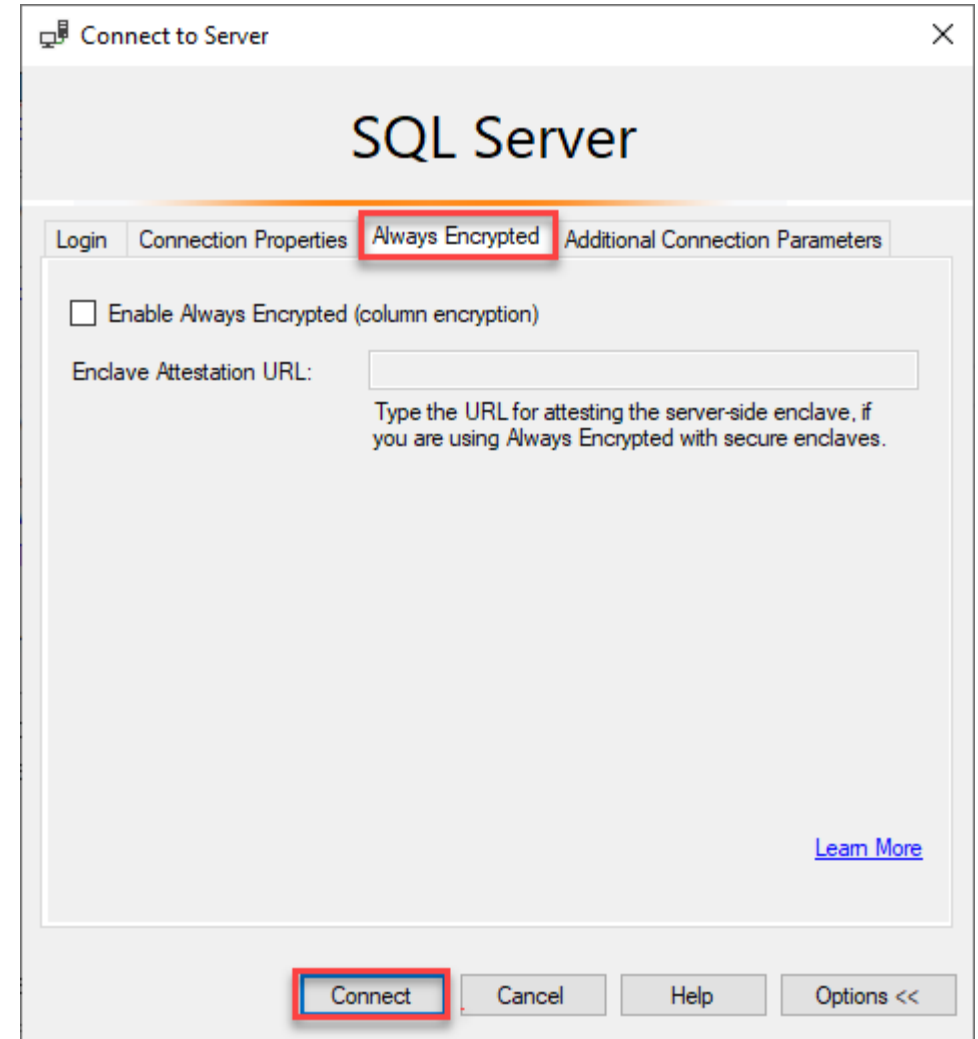


DECRYPTION IN SSMS 18.0



**ALWAYS
ENCRYPTED**

SSMS uses .NET 4.6 so you can pass in the necessary encryption options. SSMS uses the connection string to access the Master Key and return the data in its decrypted format.

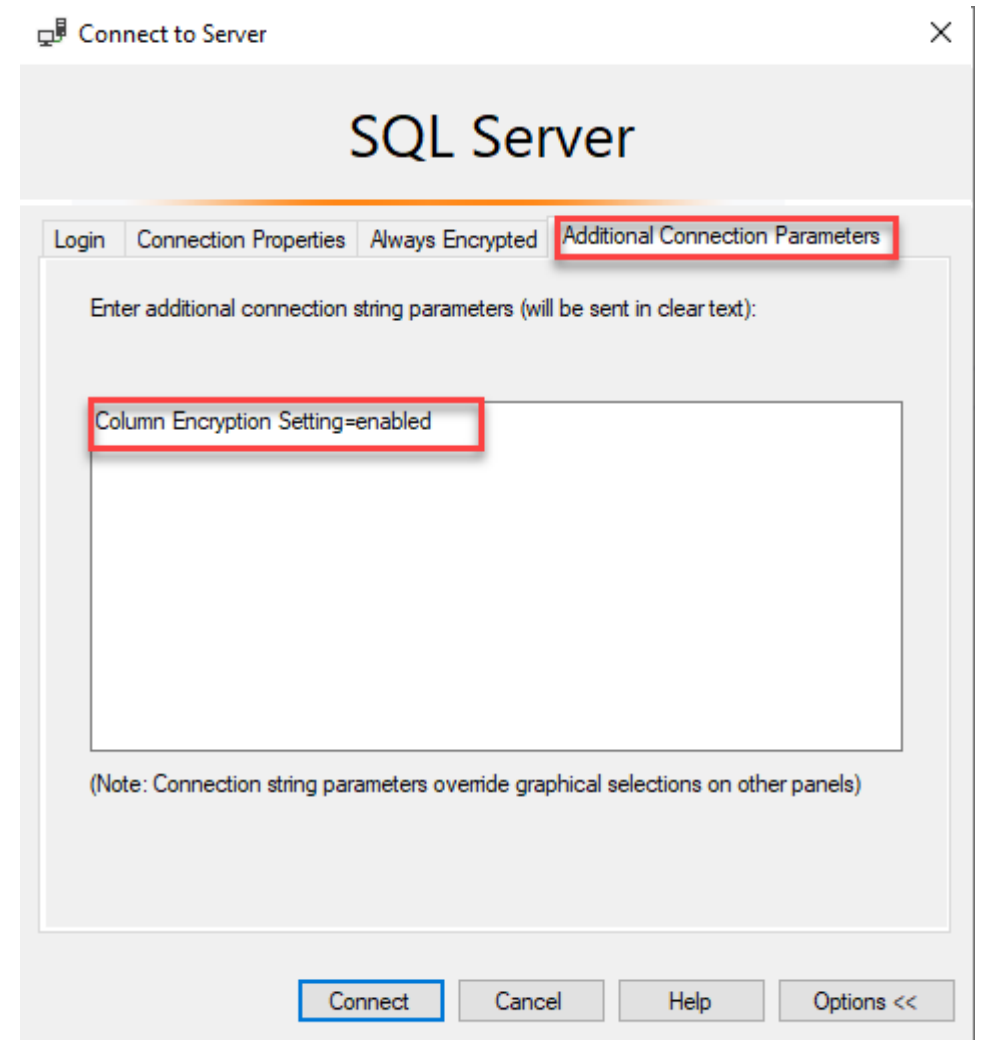


DECRYPTION IN SSMS BEFORE 18.0



**ALWAYS
ENCRYPTED**

SSMS uses .NET 4.6 so you can pass in the necessary encryption options. SSMS uses the connection string to access the Master Key and return the data in its decrypted format.



DECRYPTION IN APPLICATION

Database Permissions

*VIEW ANY COLUMN MASTER KEY
DEFINITION*

*VIEW ANY COLUMN ENCRYPTION KEY
DEFINITION*

```
string connectionString = "Data Source=server63;  
Initial Catalog=Clinic; Integrated Security=true;  
Column Encryption Setting=enabled";  
SqlConnection connection = new  
SqlConnection(connectionString);
```

These permissions are required to access the metadata about Always Encrypted keys in the database.



DECRYPTION IN APPLICATION

Database Permissions

*VIEW ANY COLUMN MASTER KEY
DEFINITION*

*VIEW ANY COLUMN ENCRYPTION KEY
DEFINITION*

```
string connectionString = "Data Source=server63;  
Initial Catalog=Clinic; Integrated Security=true;  
Column Encryption Setting=enabled"; SqlConnection  
connection = new SqlConnection(connectionString);
```

These permissions are required to access the metadata about Always Encrypted keys in the database.





DEMO

REFERENCES



MSDN

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

Secure Enclaves <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/configure-always-encrypted-enclaves?view=sqlallproducts-allversions#configure-a-secure-enclave>

TDE

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017>

Aaron Bertrand Blog

<https://blogs.sentryone.com/aaronbertrand/t-sql-tuesday-69-always-encrypted-limitations/>

ARE YOU
GOING TO
GIVE AE A TRY?

Monica Rathbun



MRathbun@sqlespresso.com



@SQLEspresso



sqlespresso.com



/in/sqlespresso



Denny Cherry
& Associates Consulting

Your Data, Our Expertise
www.dcac.com



SQL**Espresso**