# Always Encrypted

**Leonard Lobel**
CTO, SLEEK TECHNOLOGIES

@lennilobel

# Traditional SQL Server Encryption Features

**Column (cell-level) encryption**

- Uses certificates or symmetric keys

**Database (page-level) and backup encryption**

- Transparent Data Encryption (TDE)
- Uses TDE certificate with database encryption keys (DEKs)

**Keys and certificates are stored in the database**

- Risk of security breach at the database level

**Data is only encrypted “at rest”**

- Risk of security breach while “in flight”

# Introducing Always Encrypted

**Always Encrypted in SQL Server 2016**

- Based on keys managed outside the database
- Keys are never revealed to SQL Server

**Separating those who own the data from those who manage it**

- Uses client side drivers to encrypt/decrypt on the fly

**SQL server is incapable of decrypting on its own**

- Data is always encrypted in flight

**Enable Always Encrypted**

- Use T-SQL or the Always Encrypted Wizard in SSMS

# Encryption Types

**Randomized**

- Unpredictable, more secure
- No support for equality searches, joins, grouping, indexing
- Use for data that is returned but not queried

**Deterministic**

- Predictable, less secure
- Use for data that must be queried (equality support only)
- Easier to guess by examining encryption patterns
  - Increased risk for small value sets (e.g., True/False)

# Encryption Keys

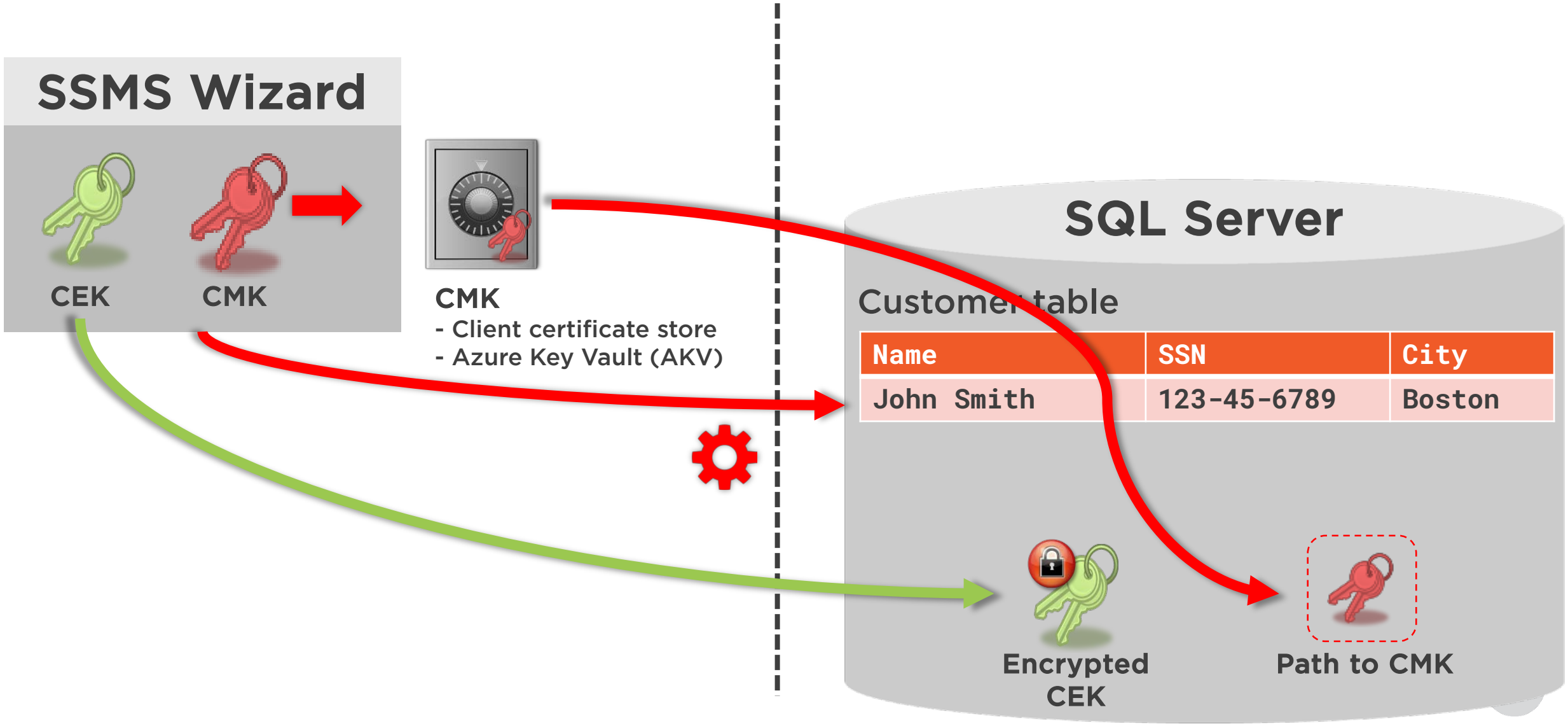
**Column Encryption Keys (CEK)**

- Used to encrypt values in specific columns
- Encrypted versions of each CEK is stored in the database

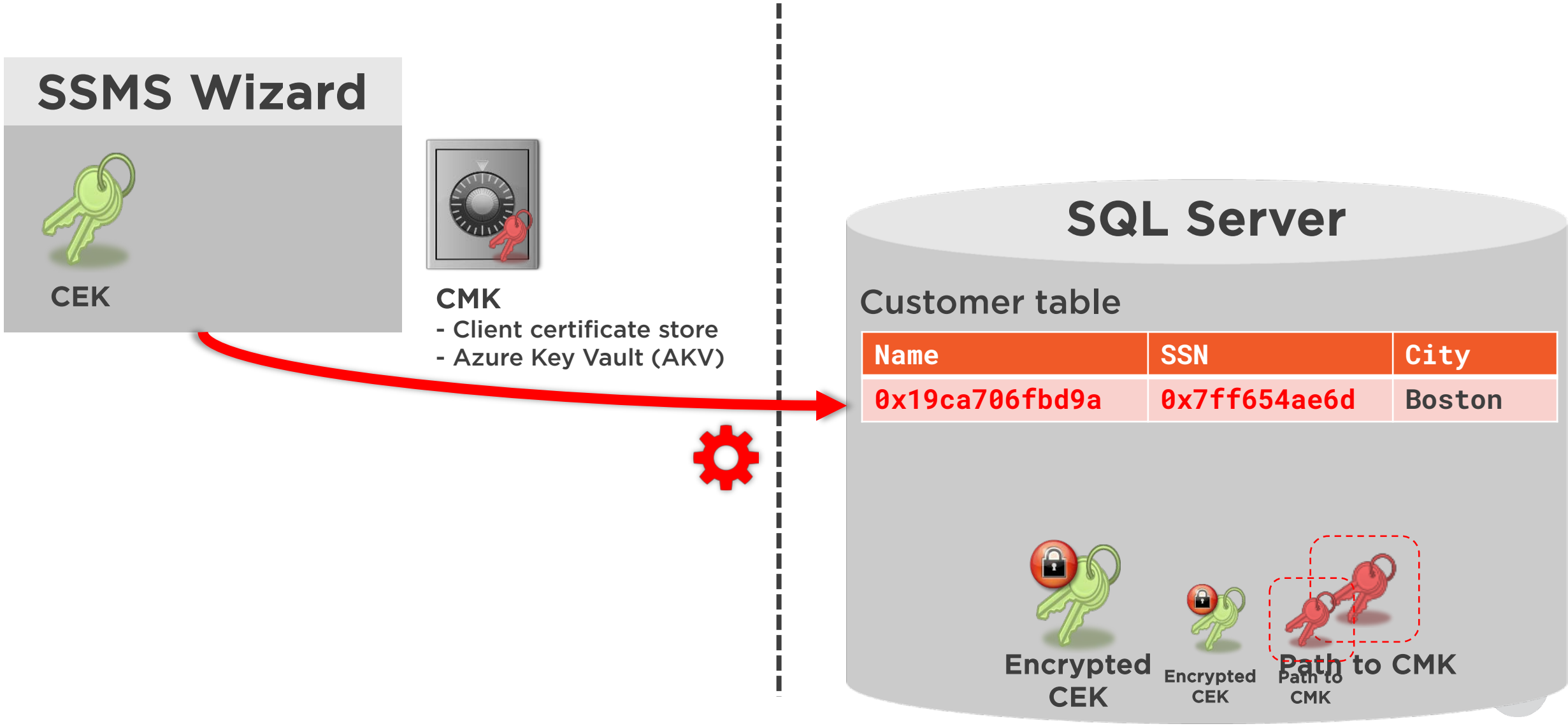
**Column Master Keys (CMK)**

- Used to encrypt all the CEKs
- Must be stored externally in a secure key store
  - Key store providers: Azure Key Vault, Certificate store, HSM

# Always Encrypted Workflow



# Always Encrypted Workflow



# Always Encrypted Workflow

## Client (your app)

Query

```
SELECT Name FROM Customer
 WHERE SSN = '123-45-6789'
```

Query result

| Name |
| --- |
| John Smith |

ADO.NET

```
SELECT Name FROM Customer
 WHERE SSN = 0x7ff654ae6d
```

## SQL Server

Customer table

| Name | SSN | City |
| --- | --- | --- |
| 0x19ca706fbd9a | 0x7ff654ae6d | Boston |

Query result

| Name |
| --- |
| 0x19ca706fbd9a |

Encrypted CEK

Path to CMK

```
Column Encryption Setting=Enabled
```

# Always Encrypted Catalog Views

**sys.column_master_keys**

- Identifies each CMK
- Contains external path to CMK location

**sys.column_encryption_keys**

- Identifies each CEK

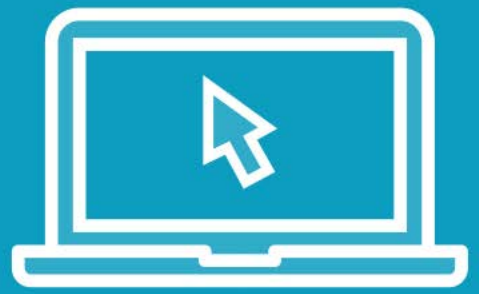
**sys.column_encryption_key_values**

- Contains CMK-encrypted values of each CEK

**sys.columns**

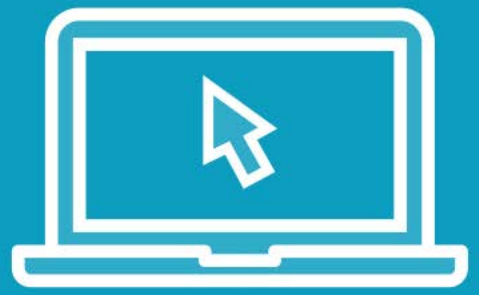
- New metadata columns to identify encrypted columns

# Demo



## Encrypting an Existing Table

# Demo



## Querying and Storing Encrypted Data

# CMK Rotation

**CEKs encrypt all your sensitive data**

- Which is why they are encrypted by a CMK

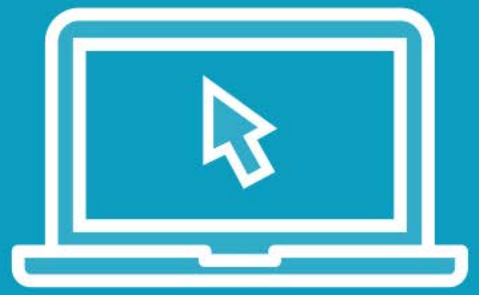
**The CMK encrypts all your CEKs**

- When the CMK is compromised, all your sensitive data is compromised

**Solution: Rotate the CMK**

- Create a new CMK
- Re-encrypt the CEKs with the new CMK
- PowerShell script available at
  - https://blogs.msdn.microsoft.com/sqlsecurity/2015/08/13/always-encrypted-key-rotation-column-master-key-rotation/
- SQL Server Management Studio has integrated GUI support

# Demo



## Rotating the Column Master Key

# AE Limitations and Considerations

**Unsupported data types**

- xml, rowversion, image, ntext, text, sql_variant, hierarchyid, geography, geometry

**Also not supported for**

- FILESTREAM, ROWGUIDCOL, IDENTITY, computed, sparse, or partitioning columns
- Fulltext indexes
- Columns with default constraints
- Temporal tables
- Stretch database

# AE Limitations and Considerations (cont.)

**Entity Framework 6 considerations**

- http://blogs.msdn.com/b/sqlsecurity/archive/2015/08/27/using-always-encrypted-with-entity-framework-6.aspx

**Additional management to install certificates on all clients**

**And more...**

- http://blogs.sqlsentry.com/aaronbertrand/t-sql-tuesday-69-always-encrypted-limitations/

# Summary

**Previous SQL Server encryption features**

- Keys and certificates on the server
- Encrypted only at rest

**Always Encrypted**

- Client-side encryption

**Encryption Types**

- Randomized vs. deterministic

**Encryption Keys**

- Column master key (CMK)
- Column encryption key (CEK)

**Demos**

- SSMS Wizard
- ADO.NET client
- Key rotation