Encrypting Data within Sql Server

Tom Norman

Data Architect - KPA

Knightdale, North Carolina

Microsoft Certified Professional

Leader - PASS Virtualization Virtual Chapter

Past President - Denver Chapter

Speaker

SQL Saturday -

Raleigh, Denver, Columbus, GA., Orange County, Colorado Springs, Albuquerque, Chicago, Richmond, Spartanburg, Nashville

KPA – Company Information

- -Nationwide compliance auto industry expert on Safety, Environmental, HR & F&I
- -Colorado Headquarters
- -29 Years Experience
- -5200 + Clients
  - Dealerships, Service, Repair, Collision Centers
- -20 Offices Serving all 50 States

- Compliance products and services
  - OSHA
  - DOT
  - EPA
  - Workers' Comp
  - Background checking
  - Onboarding
  - Harassment
  - Red Flags/CIS/8300
  - Onsite inspections
  - Online and onsite training and tracking
  - And many more…

Agenda

- Company Data Breaches
- Government Regulations
- Types of Sql Server Encryption
- Transparent Data Encryption
- Cell Level Encryption
- Always Encrypted
- Dynamic Data Masking
- Row Level Security

Company Data Breach

- Anthem Blue Cross - 80 Million, 2014
- Ashley Madison - 33 Million, 2015
- Ebay - 145 Million, 2014
- JP Morgan Chase - 76 Million, 2014
- Home Depot - 109 Million, 2014
- US Government - 21.5 Million, 2015
- Target - 110 Million, 2013
- Global Payments - 1.5 Million, 2012

Government Regulations

- Personal Identifiable Information (US)
- Data Protection Act (EU)
- Payment Card Industry (US)
- HIPAA (US)

Types of Sql Server Data Security

- Transparent Data Encryption
- Cell Level Encryption
- Always Encryption
- Dynamic Data Masking
- Row Level Security

Transparent Data Encryption

- Since Sql Server 2005
- Requires Enterprise Edition
- Does Not Require Application Change
- Data At Rest
  - Data Files
  - Log Files
  - Backups

Transparent Data Encryption

- Select Can See Data
- SSL has to be configured
- Secured By
  - Certificate
  - Extensible Key Management (EKM) Software
  - Hardware Security Module (HSM) Hardware

Cell-Level Encryption

- Since Sql Server 2005
- Requires Enterprise Edition
- Requires Application or Stored Procedure Change

Cell-Level Encryption

- Select Can See Data with Decryption function
- SSL has to be configured.
- Secured By
  - Certificate
  - Extensible Key Management (EKM) Software
  - Hardware Security Module (HSM) Hardware

Always Encrypted

- Azure Sql Database
- Sql Server 2016 - CTP 3
- All Editions
- Client Side Encryption - ADO.Net
- Needs .Net 4.6

Always Encrypted

- Types of Always Encrypted Data
  - Randomized - a method that encrypts data in a less predictable manner. Randomized encryption is more secure, but prevents equality searches, grouping, indexing, and joining on encrypted columns.
  - Deterministic - method which always generates the same encrypted value for any given plain text value. Using deterministic encryption allows grouping, filtering by equality, and joining tables based on encrypted values, but can also allow unauthorized users to guess information about encrypted values

Always Encrypted

- Secured By
  - Column Master Key-
    - Protects column encryption keys.
    - Must be stored in a trusted key store.
    - Stored in the database in system catalog views.

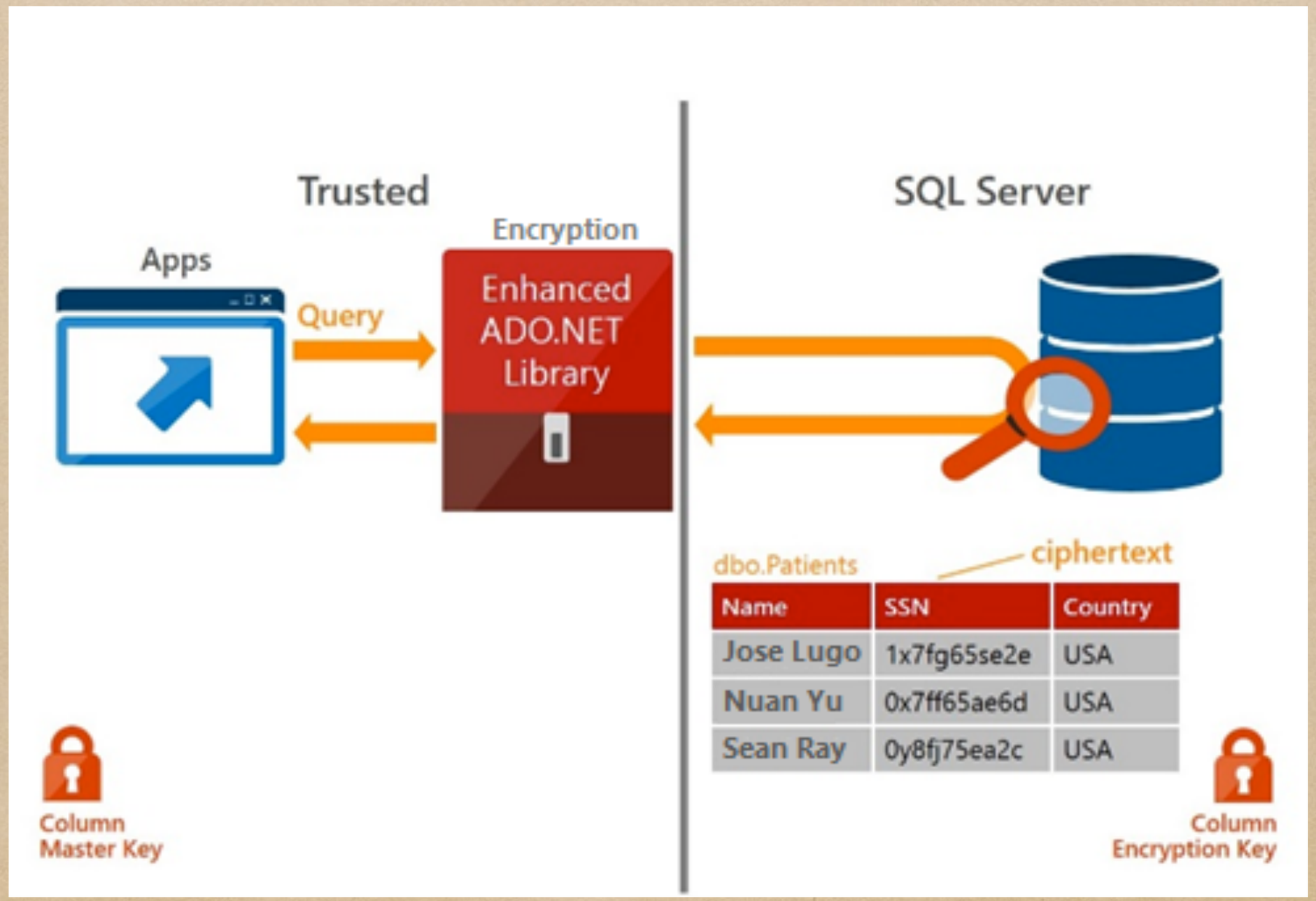
Always Encrypted

- Secured By
  - Column Encryption Key-
    - Encrypt sensitive data stored in database columns.
    - Column can be encrypted using a single column encryption key.
    - Encrypted values of column encryption keys are stored in the database in system catalog views.
    - Backup column encryption keys in a secure/trusted location.

Always Encrypted

- Store Column Master Key (Application)
  - Windows Certificate Store
  - Hardware Security Module (HSM) Hardware
  - Azure Key Vault

Always Encrypted



Always Encrypted

- Replication not supported
- Linked Server not supported
- SSDT not supported
- Only Secure when database client tier is running on-premises

Always Encrypted

- SSL Encrypted
- Data Encrypted in Memory
- Select can't see data without permissions
- Missing .Net 4.6 returns varbinary field type
- Correct setup returns field type

Always Encrypted

- Can you see the data in SSMS?
  - Yes, if you have access to the key which encrypted the data
  - No, if you don't have access to the key
  - How, add this string to your connect, column encryption setting = enabled.

Always Encrypted

BCP

Scenario	Source Schema	Target Schema	Source Settings		Target Settings	
			Column encryption setting	Allow Encrypted Values Modifications	Column encryption setting	Allow Encrypted Values Modifications
Encrypt data on migration	Plaintext	Encrypted	Any (Disabled is recommended)	N/A (OFF is recommended)	Enabled	OFF
Decrypt data on migration	Encrypted	Plaintext	Enabled	N/A (OFF is recommended)	N/A (Disabled is recommended)	N/A (OFF is recommended)
Re-encrypt data on migration	Encrypted	Encrypted	Enabled	N/A (OFF is recommended)	Enabled	OFF
Copy data without decrypting	Encrypted	Encrypted	Disabled	N/A (OFF is recommended)	Disabled	ON

```
ALTER USER Bob WITH
ALLOW_ENCRYPTED_VALUE_MODIFICATIONS = ON;
```

Dynamic Data Masking

- Sql Azure Database
- Sql Server 2016
- All Editions
- Can't Use With Always Encrypted Columns

Dynamic Data Masking

- Mask Data That Can Be Viewed
- See Entire Field With Unmasked Rights
- Where Clause Queries works as normal

Row-Level Security

- Sql Azure Database
- Sql Server 2016
- All Editions
- Issues When App Uses One User Account

Row-Level Security

- Limits the data a user is allowed to access
  - Includes Select, Insert, Update and Delete.

Resources

- Always Encrypted
  - https://msdn.microsoft.com/en-us/library/mt163865.aspx
- Dynamic Data Masking
  - https://msdn.microsoft.com/en-us/library/mt130841.aspx

Resources

- Row Level Security
- https://msdn.microsoft.com/en-us/library/dn765131.aspx

Contact Info

Tom Norman

ArmorDba@gmail.com

Twitter: @ArmorDba

LinkedIn: www.linkedin.com/in/armordba

Blog: http://armordba.wordpress.com