Encrypting Data within SQL Server
Data Architect – KPA
Raleigh, North Carolina

2018 KPA Technology Employee of the Year

Microsoft Certified Professional

PASS Virtualization Virtual Group Leader

SQL Saturday Speaker
Raleigh, Denver, Houston, Baltimore, Colorado Springs, Albuquerque, Chicago, Charlotte, Atlanta, Spartanburg, Jacksonville, Tampa, Boston, Columbus GA, Cleveland
Agenda

• Company Data Breaches
• Government Regulations
• Data Protection Types
• Encryption in SQL Server
• Always Encrypted
• SSIS with Always Encrypted
Company Data Breaches
Company Data Breaches

Aadhaar – 1.1 Billion, 2018
Exactis - 340 Million, 2018
Under Armour - 150 Million, 2018
MyHeritage - 92 Million, 2018
Facebook - 87 Million, 2018
Panera Bread - 37 Million, 2018
Ticketfly - 27 Million, 2018
Sacramento Bee - 19.5 Million, 2018
PumpUp – 6 Million, 2018
Saks, Lord & Taylor – 5 Million, 2018

Protect Your Credit

Lock and... TrueID

Credit Report
Government Regulations
Government Regulations

PII - Personal Identifiable Information (US)
GDPR – General Data Protection Regulation (EU)
  Google fined 50 Million Euro
PCI - Payment Card Industry (US)
HIPAA – Health Information Privacy (US)
California Consumer Privacy Act of 2018
  Effective January 1, 2020
Data Anonymization

Data anonymization is a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Data Protection Types
Types of Encryption

Transparent Data Encryption
Cell Level Encryption
Always Encrypted
Encryption in SQL Server
Encryption in SQL Server - TDE

- SQL Server 2005
- No Application Change
- Selects – See Data
- SSL - Configure

- Enterprise Edition
- Data At Rest
- Data Files
  - Log
  - Files
  - Backups
Encryption in SQL Server – Cell Level

- SQL Server 2005
- Application Change
- Enterprise Edition
- Selects – See Data with Decryption function
Encryption in SQL Server – Always Encrypted

- SQL Server 2016
- Client Side
- .Net 4.6
- Enterprise Edition (RTM)
- Standard Edition (SP1)
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.
Securing Always Encrypted

- **Column Master Key**
  - Protects column encryption keys.
  - Stored in a trusted key store.
  - System catalog views.
  - View in SSMS
Securing Always Encrypted

- Column Encryption Key
  - Protected by Column Master Key.
  - Encrypts sensitive column data.
  - Column encrypted with single column encryption key.
  - System catalog views.
  - Backup keys.
Column Master Key

- Windows Certificate Store
  - Current User
  - Local Machine
- Azure Key Vault
- Key Storage Provider
Always Encrypted

- SSL Encrypted
- Data Encrypted in Memory
- No DML without permissions
- Missing .Net 4.6 returns varbinary field type
- Correct setup returns field type
Always Encrypted

- See data in SSMS
  - Yes, Access to Column Master Key
  - No, no access to Column Master Key
  - Connection string parameter
    - Column Encryption Setting = Enabled
- Query Option
  - Parameterization for Always Encrypted
Always Encrypted Limitations - 2016

- Not Allowed
  - Order By
  - Cast / Convert
  - Temp Tables
  - .Net Core CLR SQL Provider
    - Out of Band SQLClient released April 2019
Always Encrypted Limitations - 2016

- Not Allowed
  - Like
  - Range
  - Indexes
  - Check Constraints
Always Encrypted Issues - 2016

- Issues
  - Field Type vs Parameter Type
  - SSMS Wizard Slow
  - SSDT convert existing fields
  - SSDT publish profile
Always Encrypted - 2019

- Secure Enclave
  - Windows Server 2019 / Windows 10 Build 1809
  - .Net Framework 4.7.2
  - .Net Framework Data Provider for SQL Server
  - Configure Host Guardian Service in environment
  - Register service hosting SQL Server
Always Encrypted - 2019
<table>
<thead>
<tr>
<th>Operation</th>
<th>Column is NOT enclave-enabled</th>
<th>Column is NOT enclave-enabled</th>
<th>Column is enclave-enabled</th>
<th>Column is enclave-enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Randomized encryption</td>
<td>Deterministic encryption</td>
<td>Randomized encryption</td>
<td>Deterministic encryption</td>
</tr>
<tr>
<td>In-place encryption</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Equality comparison</td>
<td>Not Supported</td>
<td>Supported outside of the enclave</td>
<td>Supported (inside the enclave)</td>
<td>Supported outside of the enclave</td>
</tr>
<tr>
<td>Comparison operators beyond equality</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>LIKE</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>
SSIS with Always Encrypted
Use ADO Net connection strings
Connection Manager Properties
Enable Column Encryption Setting
ALTER USER Bob
WITH ALLOW_ENCRYPTED_VALUE_MODIFICATIONS = ON;

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Source Schema</th>
<th>Target Schema</th>
<th>Source Settings</th>
<th>Target Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt data on migration</td>
<td>Plaintext</td>
<td>Encrypted</td>
<td>Any (Disabled is recommended)</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A (OFF is recommended)</td>
<td>OFF</td>
</tr>
<tr>
<td>Decrypt data on migration</td>
<td>Encrypted</td>
<td>Plaintext</td>
<td>Enabled</td>
<td>N/A (OFF is recommended)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A (Disabled is recommended)</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A (OFF is recommended)</td>
<td>OFF</td>
</tr>
<tr>
<td>Re-encrypt data on migration</td>
<td>Encrypted</td>
<td>Encrypted</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A (OFF is recommended)</td>
<td>OFF</td>
</tr>
<tr>
<td>Copy data without decrypting</td>
<td>Encrypted</td>
<td>Encrypted</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A (OFF is recommended)</td>
<td>ON</td>
</tr>
</tbody>
</table>
What Column Do I Encrypt?
What Column Do I Encrypt?

- First Name
- Last Name
- Name
- Birthdate
- Address
- Email
- Phone
- Tax Id Number
- Driver’s License Number
- Medical Evaluation Notes
- MAC Address
- IP Address
What Column Do I Encrypt?

- First Name - No
- Last Name – No
- Name - Yes
- Birthdate - No
- Address - No
- Email - Yes
- Phone - Yes
- Tax Id Number - Yes
- Driver’s License Number - Yes
- Medical Evaluation Notes – Yes
- MAC Address – No
- IP Address - No
References

TDE - Setup
https://sqlserverstore.blogspot.com/2016/02/how-to-configure-and-remove-transparent.html

Always Encrypted - Features
References

Always Encrypted – SSMS Modify Data

Always Encrypted – SQL Server 2019
References

GDPR Guidelines

https://t.co/mwU1K9MzFl?amp=1

Questions
Demo