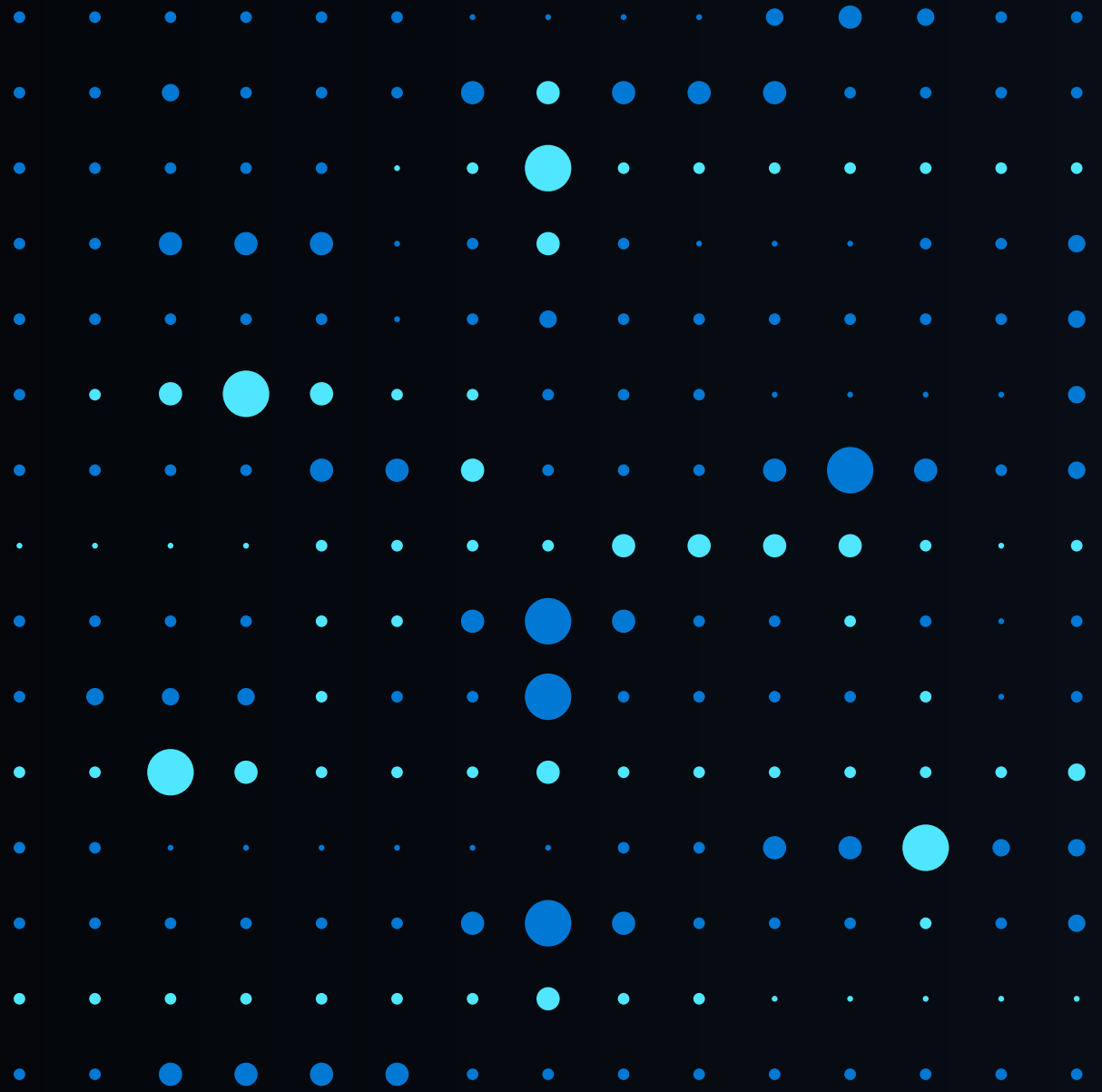
Microsoft



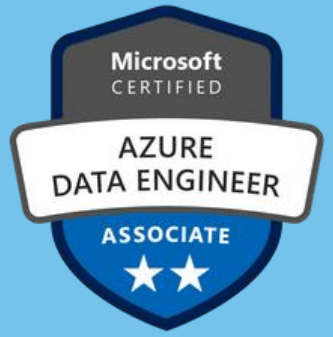
Getting Started: SQL Server Data Security

John Deardurff

John Deardurff

Microsoft Customer Engineer (Global Technical Team)
Microsoft Certified Trainer (Regional Lead)
MVP: Data Platform (2016 – 2018)

Email: John.Deardurff@Microsoft.com
Twitter: @SQLMCT
Website: www.SQLMCT.com
GitHub: github.com\SQLMCT



What does this session cover?

- What is Row Level Security
- What is Dynamic Data Masking
- What is Always Encrypted?
- Demonstration

Row Level Security

A security feature that will restrict access to specific rows in a table based on values in a column.

Row Level Security Scenarios

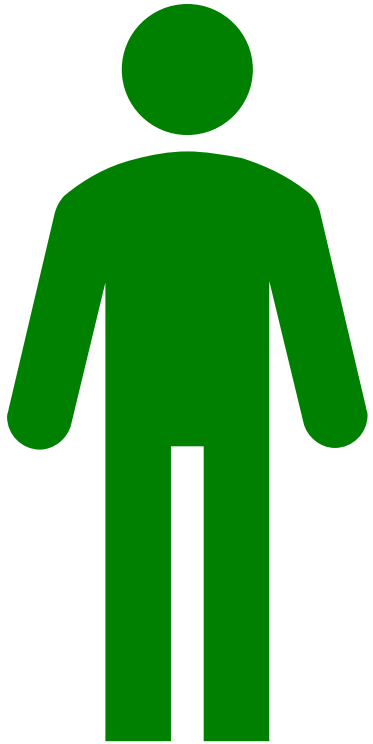
A hospital can restrict doctors and nurses to only view data about their specific patients.

A bank can restrict access to data based on the location of their branch offices.

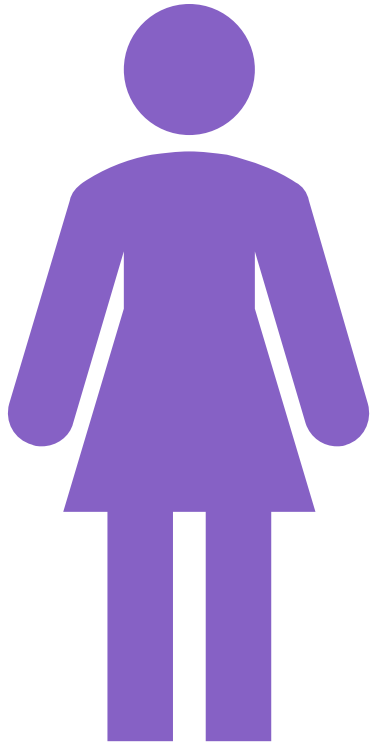
A bicycle company can restrict sales leads to only specific salespeople.

Salespeople for the Adventure Works Bicycle Company

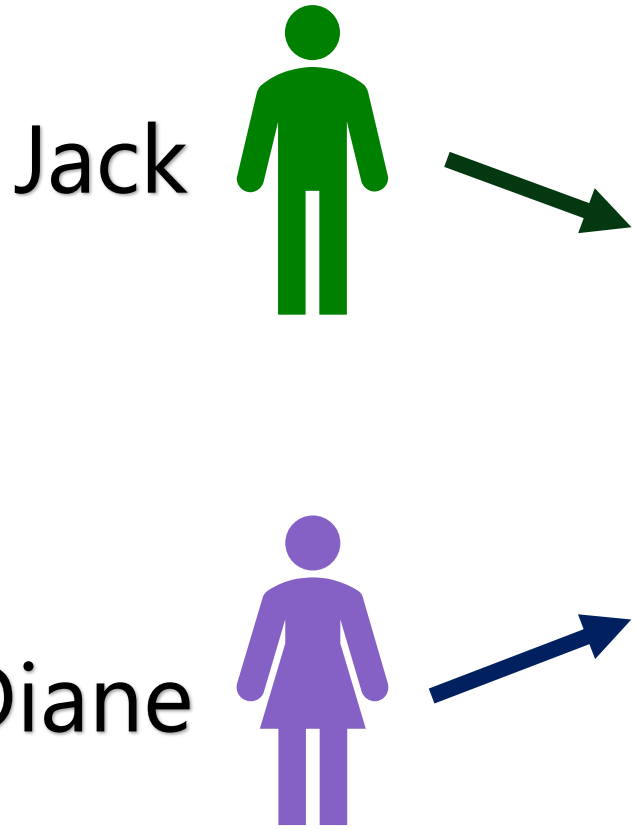
Jack



Diane



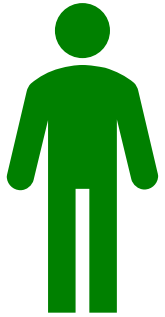
Salespeople for the Adventure Works Bicycle Company



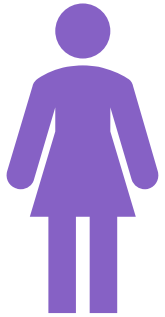
CustomerName	CustomerEmail	SalesPersonName
Stephen Jiang	Stephen.Jiang@adworks.com	Jack
Michael Blythe	Michael@contoso.com	Jack
Linda Mitchell	Linda@VolcanoCoffee.org	Jack
Jilian Carson	JilianC@Northwind.net	Jack
Garret Vargas	Garret@WorldWideImporters.com	Diane
Shu Ito	Shu@BlueYonder.com	Diane
Sahana Reiter	Sahana@CohoVines.com	Diane
Syed Abbas	Syed@AlpineSki.com	Diane

Salespeople for the Adventure Works Bicycle Company

Jack



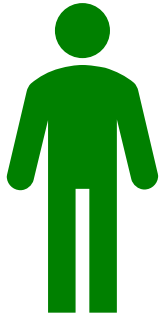
Diane



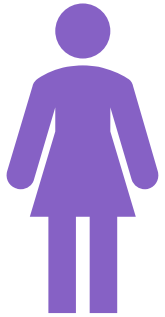
CustomerName	CustomerEmail	SalesPersonName
Stephen Jiang	Stephen.Jiang@adworks.com	Jack
Michael Blythe	Michael@contoso.com	Jack
Linda Mitchell	Linda@VolcanoCoffee.org	Jack
Jilian Carson	JilianC@Northwind.net	Jack
Garret Vargas	Garret@WorldWideImporters.com	Diane
Shu Ito	Shu@BlueYonder.com	Diane
Sahana Reiter	Sahana@CohoVines.com	Diane
Syed Abbas	Syed@AlpineSki.com	Diane

Salespeople for the Adventure Works Bicycle Company

Jack



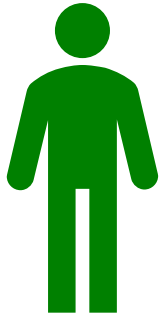
Diane



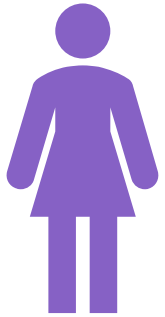
CustomerName	CustomerEmail	SalesPersonName
Stephen Jiang	Stephen.Jiang@adworks.com	Jack
Michael Blythe	Michael@contoso.com	Jack
Linda Mitchell	Linda@VolcanoCoffee.org	Jack
Jilian Carson	JilianC@Northwind.net	Jack
Garret Vargas	Garret@WorldWideImporters.com	Diane
Shu Ito	Shu@BlueYonder.com	Diane
Sahana Reiter	Sahana@CohoVines.com	Diane
Syed Abbas	Syed@AlpineSki.com	Diane

Salespeople for the Adventure Works Bicycle Company

Jack



Diane



CustomerName	CustomerEmail	SalesPersonName
Stephen Jiang	Stephen.Jiang@adworks.com	Jack
Michael Blythe	Michael@contoso.com	Jack
Linda Mitchell	Linda@VolcanoCoffee.org	Jack
Jilian Carson	JilianC@Northwind.net	Jack
Garret Vargas	Garret@WorldWideImporters.com	Diane
Shu Ito	Shu@BlueYonder.com	Diane
Sahana Reiter	Sahana@CohoVines.com	Diane
Syed Abbas	Syed@AlpineSki.com	Diane

Demonstration

Dynamic Data Masking

A security feature that will restrict unauthorized users from viewing sensitive data

Dynamic Data Masking Scenarios

Developers can troubleshoot production data without viewing sensitive information.

Customer Service representatives can view parts of sensitive data like credit card information.

Reports can be distributed with sensitive data obfuscated.

Dynamic Data Masking Functions

Default

Random

Custom

Email

Dynamic Data Masking Functions

Default

The default function of Dynamic Data Masking masks data based on the column's data type.

Data and Time – 1900-01-01 00:00:00.000

Numeric – 0

String – Adds maximum of 4 X’s

Dynamic Data Masking Functions

Random

The Random Data Masking function is only applied on numeric data types. It displays a random value for the specified range.

Dynamic Data Masking Functions

Custom

The Custom masking function allows the ability to create a custom mask using the Partial function.

Syntax : Partial(prefix,[padding],suffix)

Prefix – Starting characters to display.
Padding –Custom string for masking.
Suffix – Last characters to be displayed.

Dynamic Data Masking Functions

Email

The email masking function will display the first character of an email address and will then mask the rest of the address with XXX@XXXX and will include the .com email suffix.

Example: JXXX@XXXX.com

Dynamic Data Masking Functions

Default

Random

Custom

Email

Demonstration

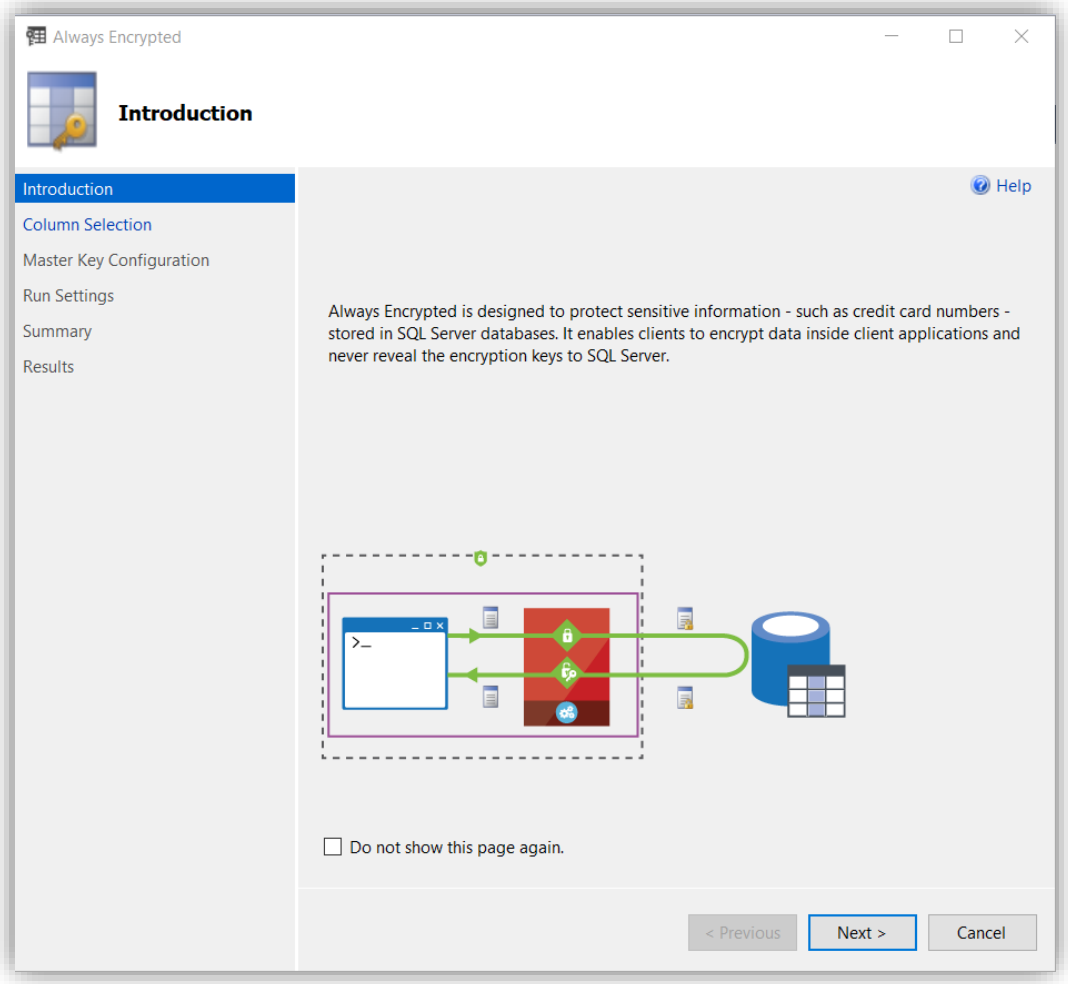

Always Encrypted

What is Always Encrypted?

Allows encrypting specific columns

Client-side encryption/decryption

Based on certificate stored on client machines



Benefits

Allows customers to securely store sensitive data outside of their trust boundary while protecting data from highly privileged users.

Prevention of data disclosure

- Client-side encryption of sensitive data using keys that are never given to database system.

Queries on encrypted data

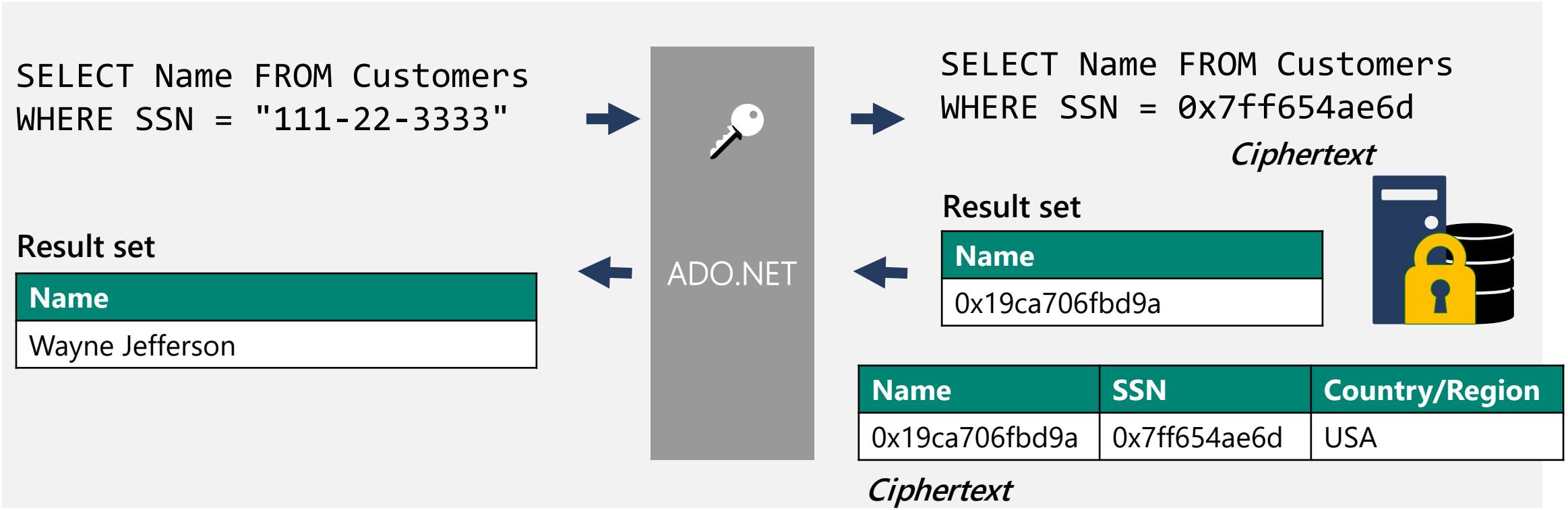
- Support for equality comparison, including join, group by, and distinct operators

Application transparency

- Minimal application changes through server and client library enhancements

How does Always Encrypted work?

Encrypted sensitive data and corresponding keys are never seen in plain text in SQL Server



Column Keys

CMK – Column Master Key is used to encrypt other keys, always in client's control, and in an external key store

- Azure Key Vault
- Windows Certificate Store
- Hardware Security Sections

CEK – Column Encryption Key is a content encryption key

Encryption Methodologies

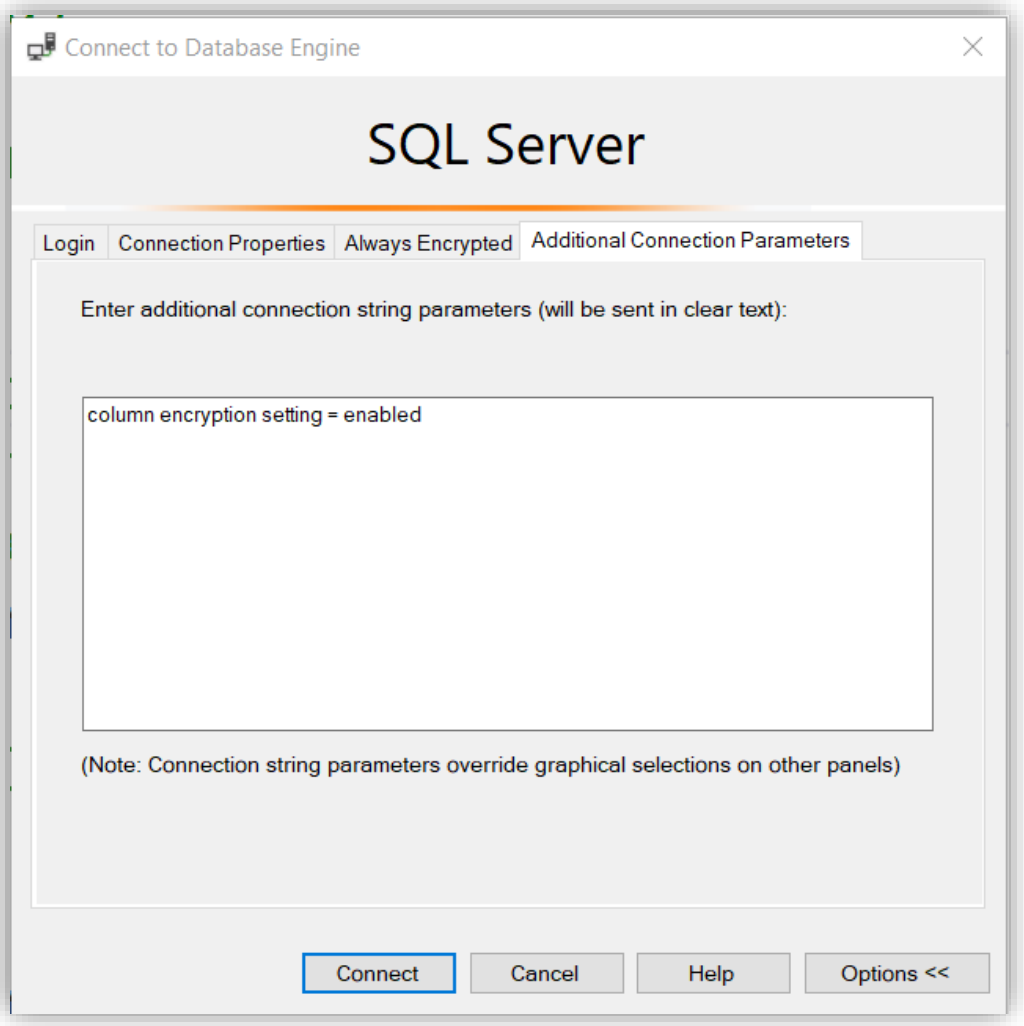
Randomized encryption

- Encrypt ('123-45-6789') = 0x0123A99C
- Repeat: Encrypt ('123-45-6789') = 0x01EB449B

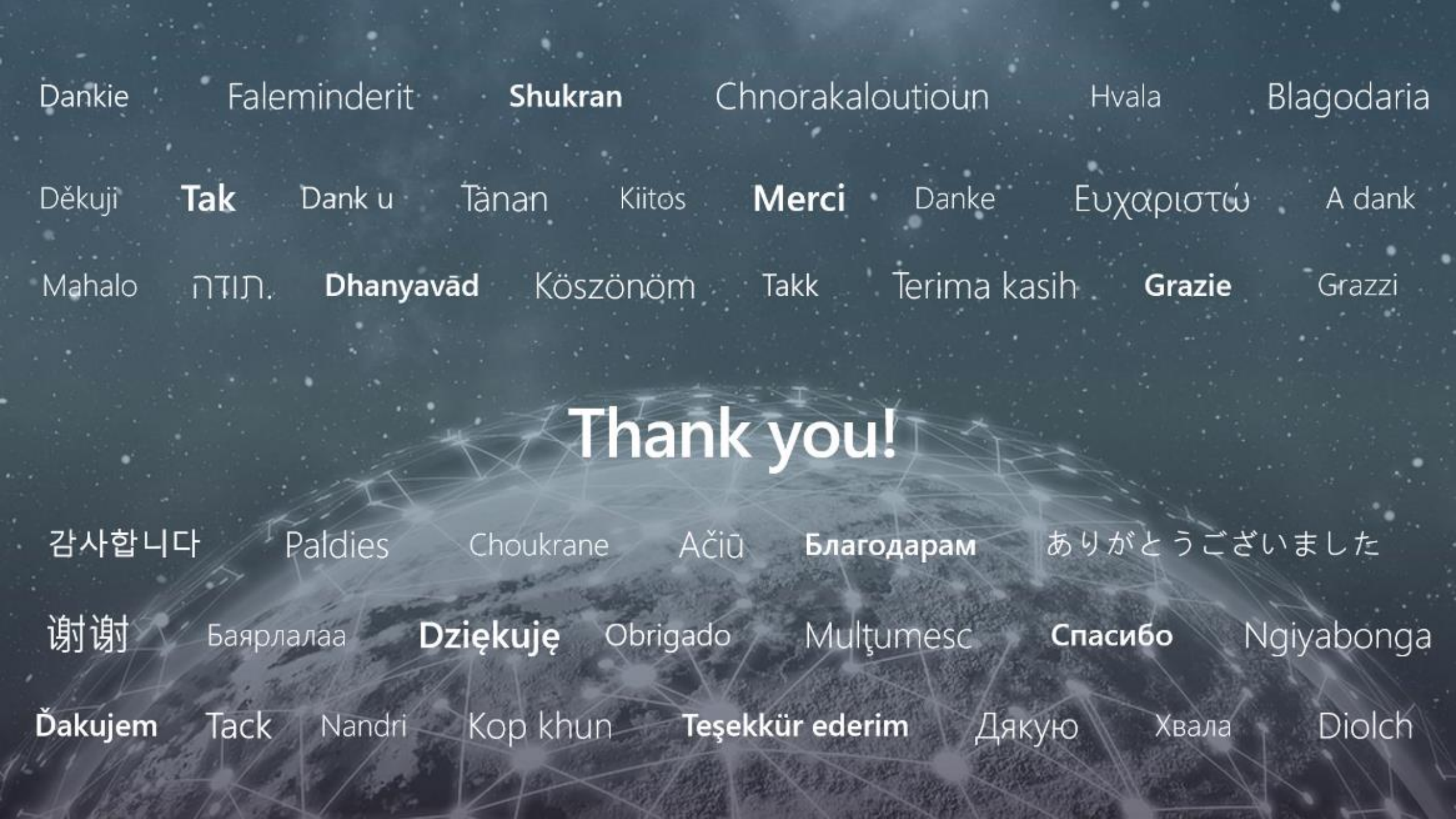
Deterministic encryption

- Encrypt ('123-45-6789') = 0x17cfd50a
- Repeat: Encrypt ('123-45-6789') = 0x17cfd50a

Column Encryption Setting = Enabled



Demonstration


Dankie
Faleminderit
Shukran
Chnorakaloutioun
Hvala
Blagodaria
Děkuji
Tak
Dank u
Tänan
Kiitos
Merci
Danke
Ευχαριστώ
A dank
Mahalo
תודה.
Dhanyavād
Köszönöm
Takk
Terima kasih
Grazie
Grazzi
Thank you!
감사합니다
Paldies
Choukrane
Ačiū
Благодарам
ありがとうございました
谢谢
Баярлалаа
Dziękuję
Obrigado
Mulţumesc
Спасибо
Ngiyabonga
Ďakujem
Tack
Nandri
Kop khun
Teşekkür ederim
Дякую
Хвала
Diolch