SQL KONFERENZ 2025

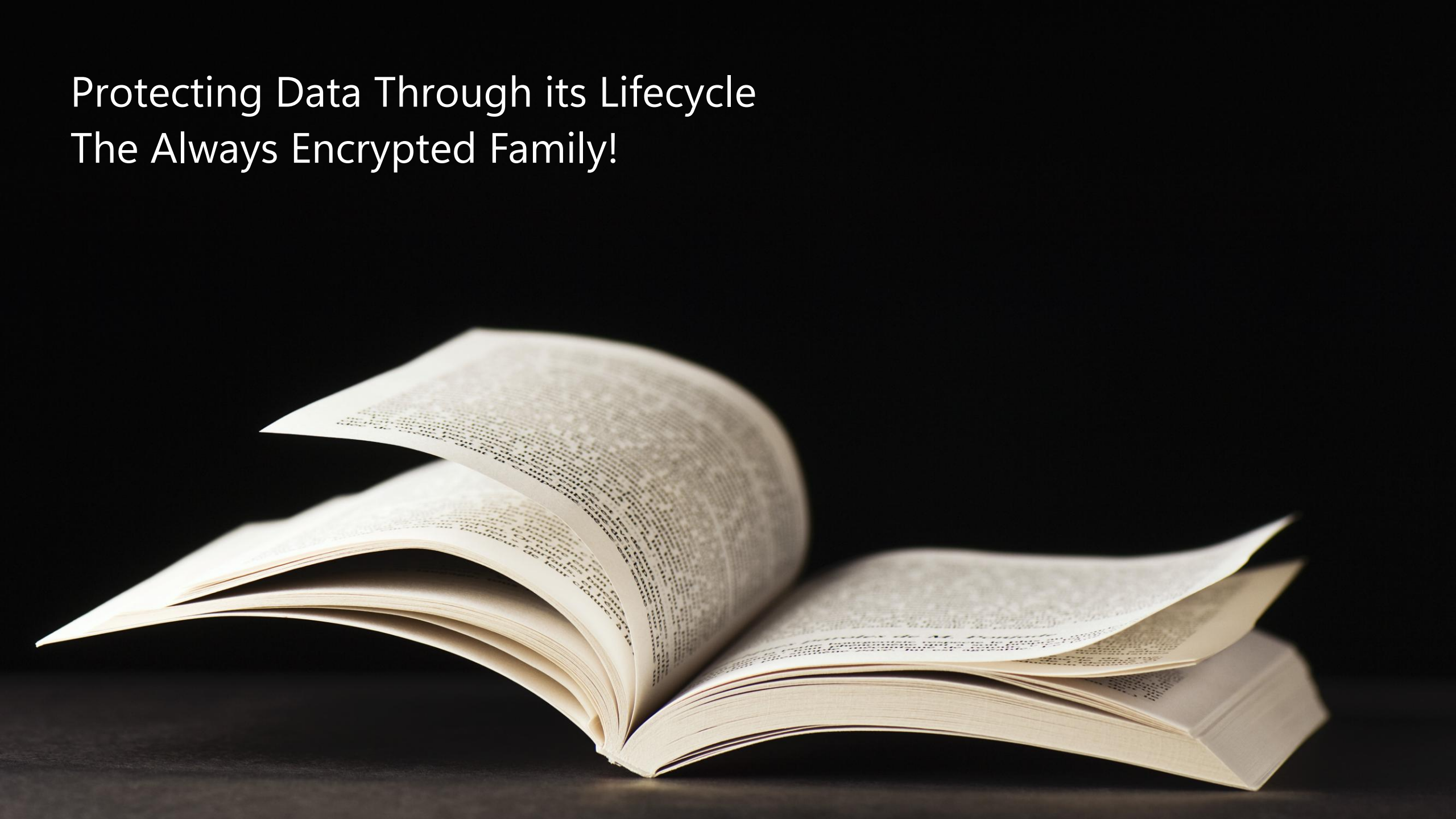


Confidential computing with Always Encrypted using enclaves

Pieter Vanhove

Senior Program Manager - Microsoft

Protecting Data Through its Lifecycle
The Always Encrypted Family!



Protecting Data Through its Lifecycle

Protecting Data Through its Lifecycle

EXISTING ENCRYPTION



Data at rest

Encrypt inactive data when stored in database files, backup files, log files

Transparent Database Encryption (TDE)



Data in transit

Encrypt data that is flowing between applications and the database

Transport Layer Security (TLS)

Protecting Data Through its Lifecycle

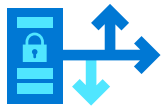
EXISTING ENCRYPTION



Data at rest

Encrypt inactive data when stored in database files, backup files, log files

Transparent Database Encryption (TDE)



Data in transit

Encrypt data that is flowing between applications and the database

Transport Layer Security (TLS)

CONFIDENTIAL COMPUTING



Data in use

Encrypt data used during query processing

Always Encrypted

The Always Encrypted Family!

Motivation

Enable customers to confidently store their most sensitive data in the cloud

Customers can stay in control of their data

Protect sensitive data in use from high-privileged yet unauthorized users

Traditional access control (SQL permissions, RBAC) and encryption technologies (TDE/TLS) are insufficient

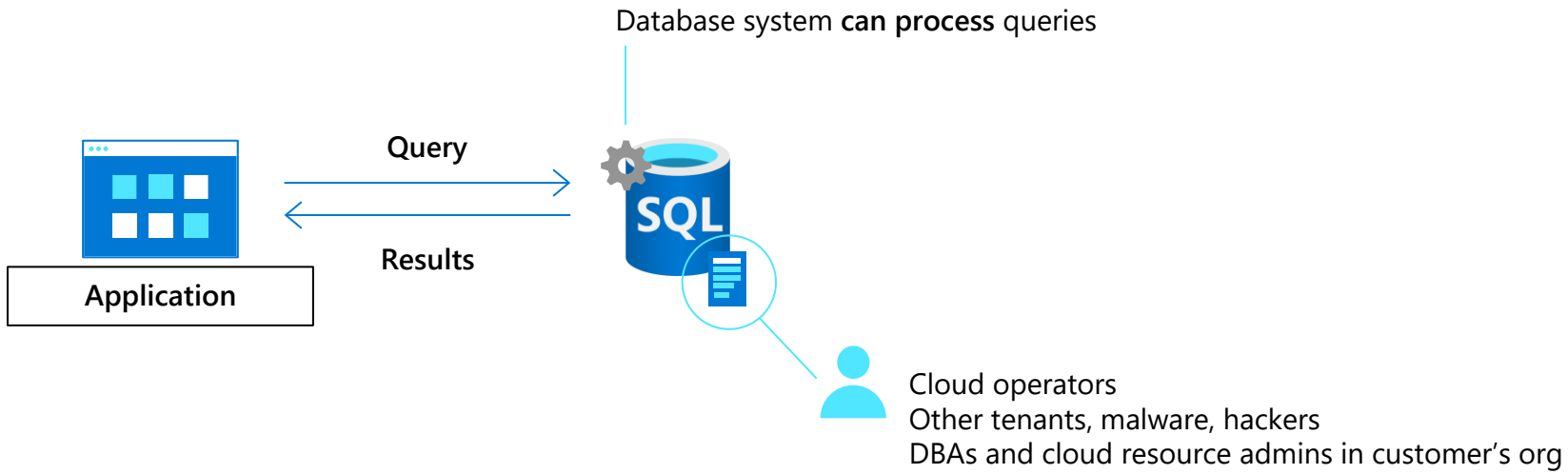
Third-party client-side encryption solutions make it impossible to query and process the protected data in the cloud

Support confidential computations

Query processing without exposing data to admins

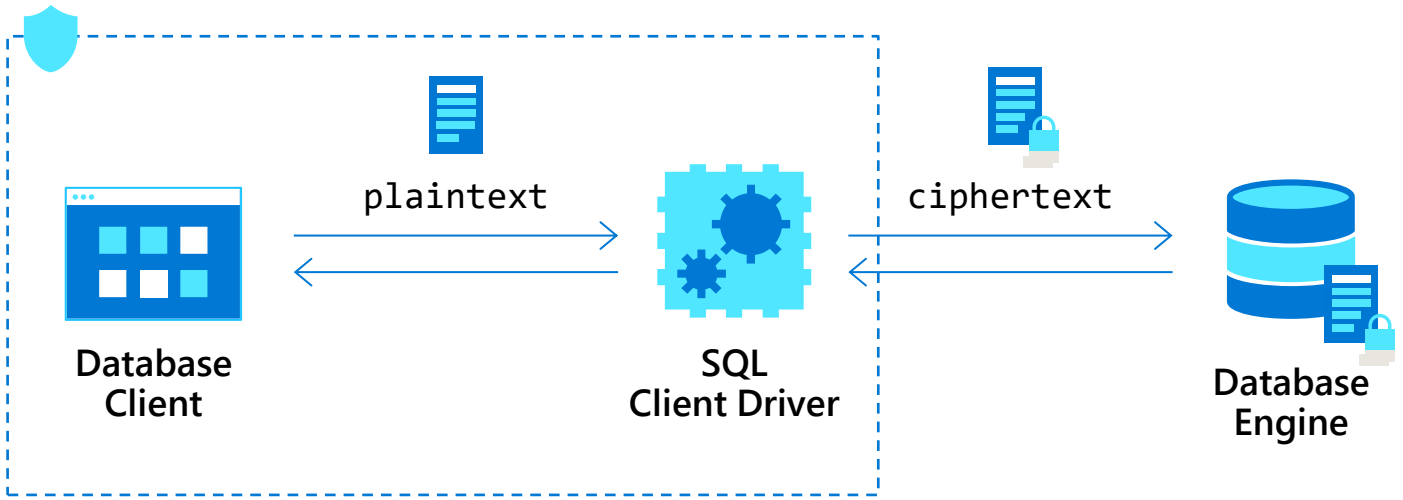
Support Zero Trust Initiatives

In a Zero Trust “Assume Breach” scenario, the attacker does NOT have access to the data encryption keys



Always Encrypted

Protects data in-use from malicious DBAs, OS admins, and malware



Client-side encryption

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

Encryption transparency

Client driver transparently encrypts query parameters and decrypts encrypted results

Confidential equality comparisons

Point lookup searches, equality joins, grouping via deterministic encryption

Example

Client - trusted

```
using (SqlCommand cmd =
new SqlCommand(
  "SELECT Name, SSN FROM Customers
      WHERE SSN = @SSN", conn)) {
   cmd.Parameters.Add(new
  SqlParameter(
     "@SSN",
     SqlDbType.VarChar,11).Value
       = "111-22-3333");
 SqlDataReader reader =
  cmd.ExecuteReader();
}
```



Trust Boundary

Azure SQL/SQL Server - untrusted

Plaintext CEK Cache



Client Driver

All encryption and decryption performed here

```
EXEC sp_describe_parameter_encryption
@params = N'@SSN VARCHAR(11)',@tsql =
N'SELECT Name, SSN FROM Customers WHERE SSN = @SSN'
```

```
Encryption metadata for the parameters that
correspond to encrypted columns using
sp_describe_parameter_encryption
```

```
EXEC sp_execute_sql
N'SELECT Name, SSN FROM Customers WHERE SSN = @SSN'
, @params = N'@SSN VARCHAR(11)', @SSN=0x01f654ae6d...
```

```
Name=Jim Gray; SSN=0x01f654ae6d...
```

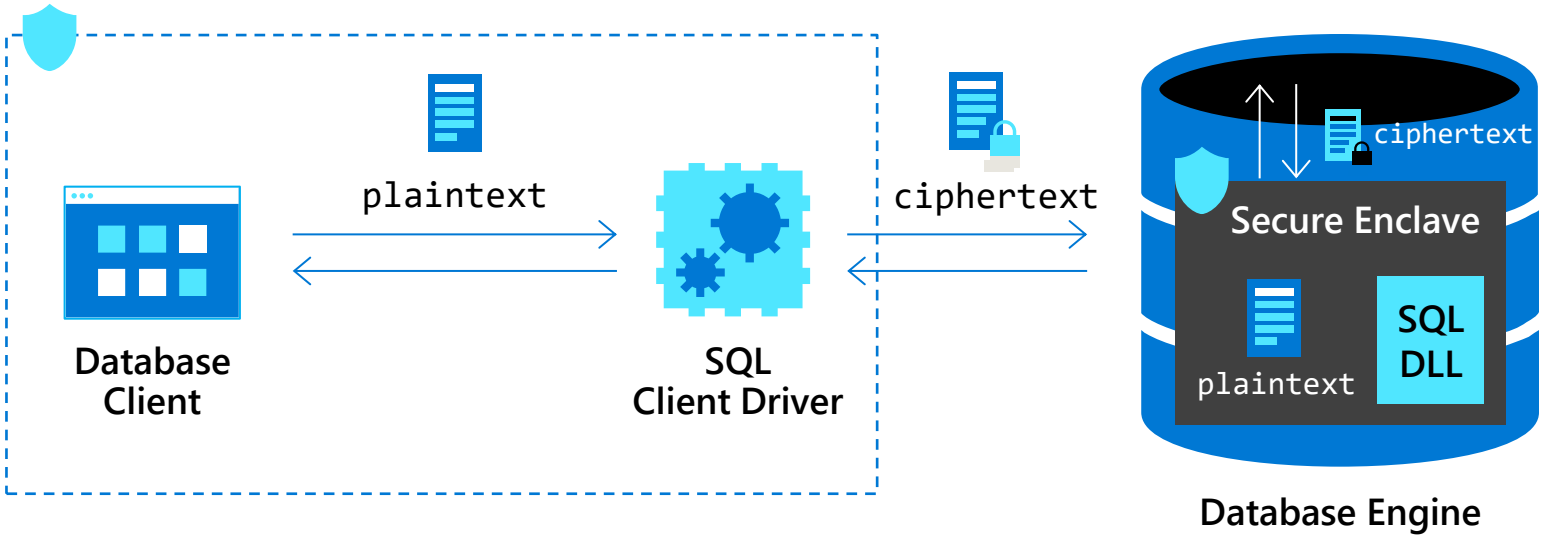
Result set

Name	SSN
Jim Gray	111-22-3333

Not encrypted

Decrypted by client driver

Always Encrypted with secure enclaves



Secure computations inside the enclave

Database Engine delegates operations on encrypted data to the enclave, where the data can be safely decrypted and processed

Rich queries

Pattern matching (LIKE), range queries (<, >, etc.), sorting, indexing

In-place encryption

The enclave can perform initial data encryption and key rotation without moving the data out of the database

What are enclaves?

Enclave

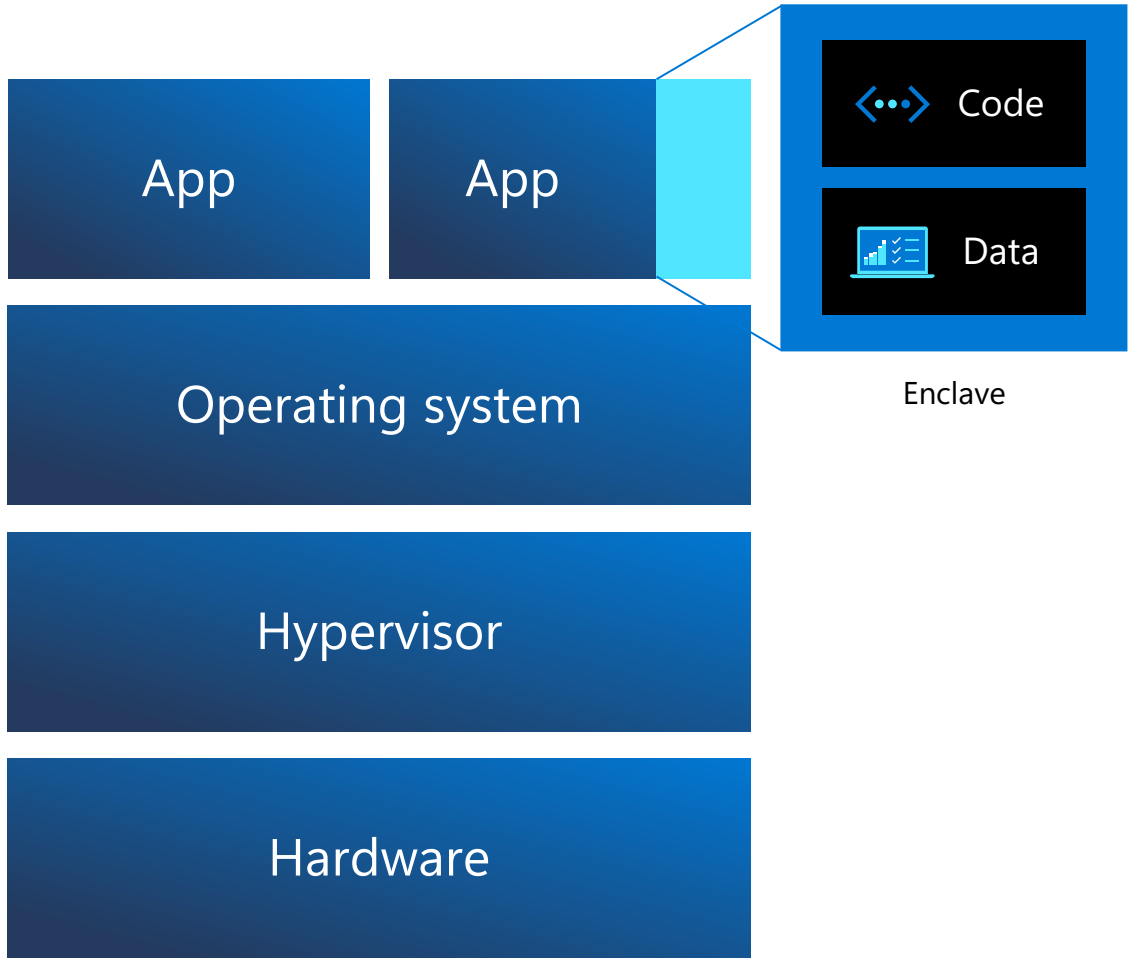
An isolated region of memory

Provides a trusted execution environment

Data stored inside the enclave cannot be accessed outside of the enclave

Secure isolation powered by:

Hardware - Software Guard Extension (Intel SGX)
Hypervisor - Virtualization-Based Security (VBS) in Windows Server 2019+, Windows 10, v. 1809+

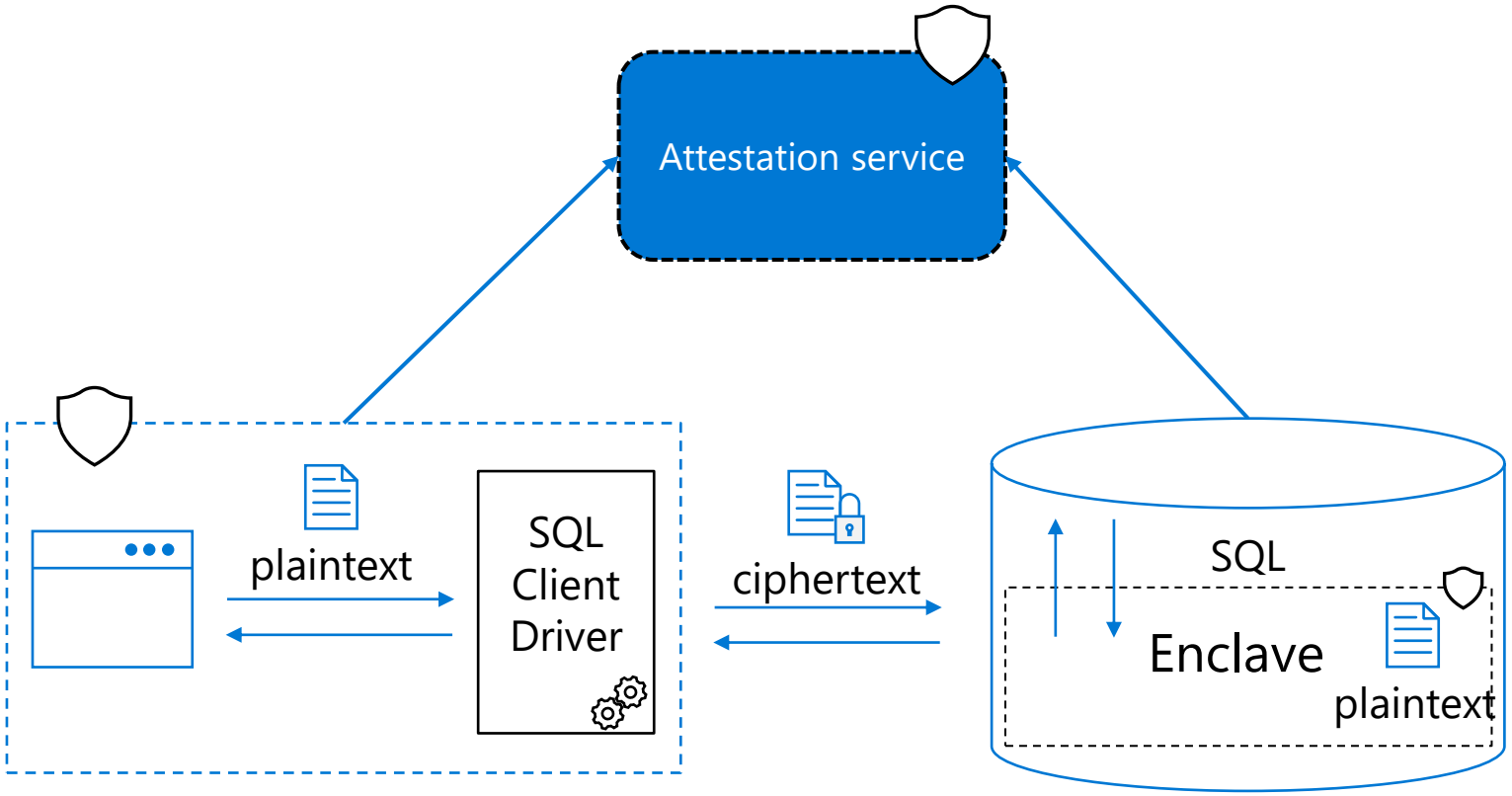


Secure Enclaves in Azure SQL Database

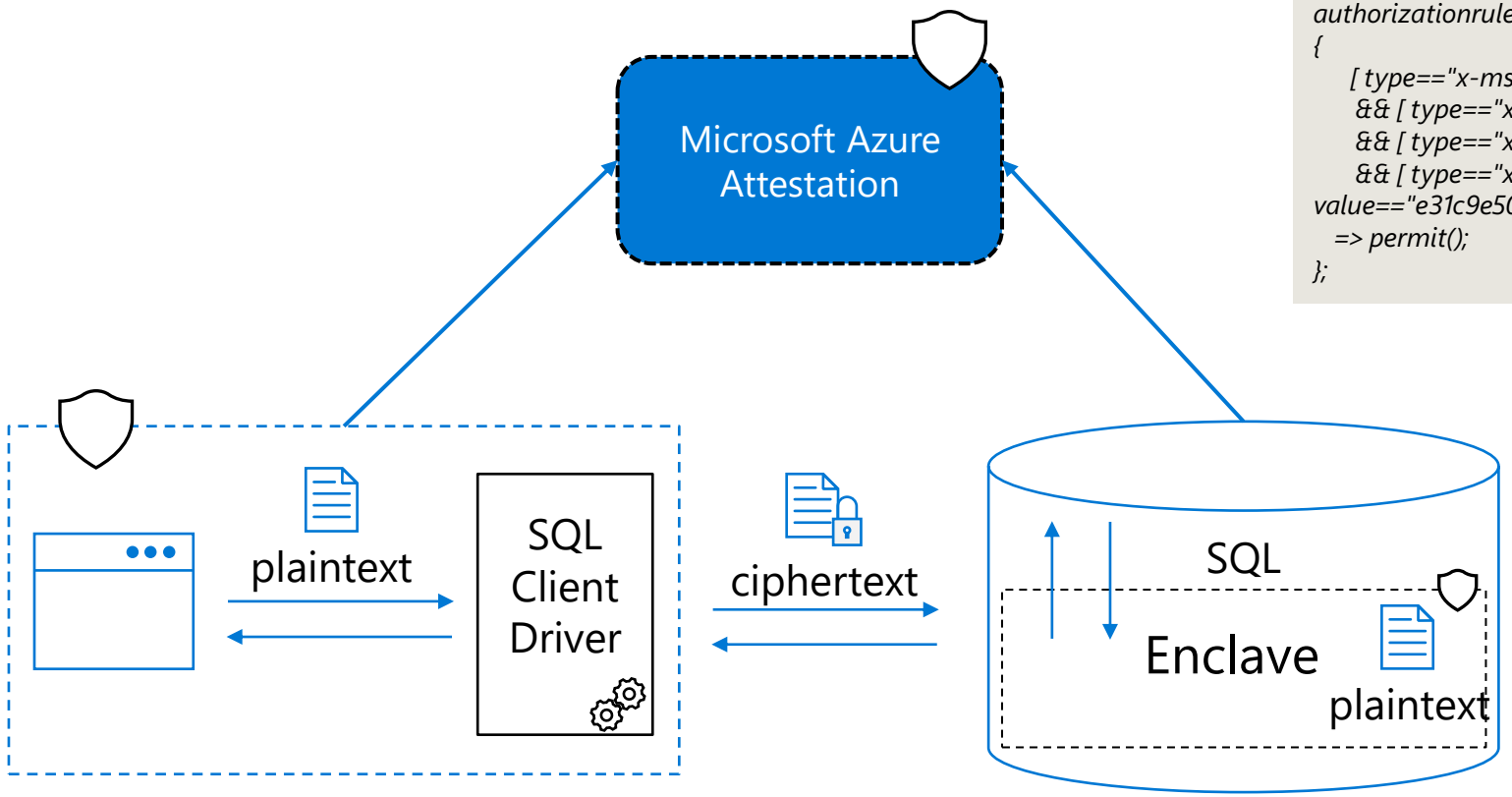
	Intel Software Guard eXtensions (SGX)	Virtualization-based security (VBS)
	Available in DC-series hardware configuration	No hardware dependency
Purchasing model	vCore model	DTU and vCore
Compute mode	Provisioned	Provisioned and serverless
Compute size	Up to 40 (physical) vCores	Any (up to 128 vCores)
Regional availability	Regional availability: East/West US, North/West EU, Canada Central, UK South, Southeast Asia	All Azure regions
Security	Protection from rogue customer's DBAs	Protection from rogue customer's DBAs
	Protection from attacks originating from both guest and host OS (rogue cloud operators, malware)	Protection from attacks originating from guest OS (rogue cloud operators, malware), but **not** host OS
	Attestation using Microsoft Azure Attestation	No attestation currently supported

Enclave Attestation

- How do you (and your app) know the enclave can be trusted?
- By using an attestation protocol and an attestation service



Attestation in Azure SQL Database Using Microsoft Azure Attestation




```
version= 1.0;
authorizationrules
{
    [ type=="x-ms-sgx-is-debuggable", value==false ]
     && [ type=="x-ms-sgx-product-id", value==4639 ]
     && [ type=="x-ms-sgx-svn", value>= 2 ]
     && [ type=="x-ms-sgx-mrsigner",
value=="e31c9e505f37a58de09335075fc8591254313eb20bb1a27e5443cc450b6e33e5"]
  => permit();
};
```

Supported attestation protocols by SQL Product

Hosting product	Enclave type	Supported attestation protocols
SQL Server 2019 (15.x) and later	VBS enclaves	HGS, No attestation
Azure SQL Database	SGX enclaves	Microsoft Azure Attestation
Azure SQL Database	VBS enclaves	No attestation

Encryption Methodologies

Two types of encryption are available:

- Randomized encryption uses method that encrypts data in less predictable manner
- Deterministic encryption uses method that always generates same encrypted value for any given plain text value

Encryption keys for both are cryptographically random AES-256 keys

Name	Zip code (Deterministic)	Zip code (Randomized)
John Davis	0x85a55d3f	0x17cfd50a
Chris Vanderbilt	**0x56v99q0x**	0x57dfr48z
Steve Verschaeve	0x85a55d3f	0x89jzs38b
Rupert Stevens	0x85a55d3f	0x22bn67s
Jacky Bertrand	**0x56v99q0x**	0x99iol31w
	Always Encrypted	Always Encrypted Always Encrypted with secure enclaves

Roles and Responsibilities

Database Administrator	Security Officer	Developer/Application Owner
Configures Azure SQL Database to use Always Encrypted with secure enclaves Manages metadata about the keys in the database	Generates column encryption keys and column master keys and manages key stores containing the column master keys.	Encrypts the columns Configures the connection string to use Always Encrypted Writes code that takes advantage of Always Encrypted

Demo - Always Encrypted using VBS enclaves in Azure SQL Database

Supported operations in DML Queries

Operation	SQL Server 2019 (15.x)	SQL Server 2022 (16.x)	Azure SQL Database
Comparison Operators	Supported	Supported	Supported
BETWEEN (Transact-SQL)	Supported	Supported	Supported
IN (Transact-SQL)	Supported	Supported	Supported
LIKE (Transact-SQL)	Supported	Supported	Supported
DISTINCT	Supported	Supported	Supported
Joins	Only nested loop joins supported	Supported	Supported
SELECT - ORDER BY Clause (Transact-SQL)	Not supported	Supported	Supported
SELECT - GROUP BY-Transact-SQL	Not supported	Supported	Supported

- Supported with randomized encryption
- Collations:
  - SQL Server 2019 requires a BIN2 collation for string columns
  - Azure SQL Database ans SQL server 2022 supports both BIN2 and UTF-8 collations
- Non-clustered indexes

Drivers and Tools

- Drivers supporting enclaves in Azure SQL Database
  - JDBC, ODBC, SqlClient
- Tools
  - Key provisioning: SSMS, PowerShell, sqlpackage.exe
  - In-place encryption: SSMS, Azure Data Studio* – only via T-SQL (ALTER TABLE)



Resources Always Encrypted

Blog Post	aka.ms/sqldb-enclaves-blog
Documentation	aka.ms/AlwaysEncryptedEnclavesAzureSQLDB
Tutorial	aka.ms/AlwaysEncryptedEnclavesAzureSQLDBTutorial
Data Exposed	aka.ms/AlwaysEncryptedEnclavesDataExposed
Always Encrypted Podcast	The Azure Security Podcast
Sample Code	aka.ms/AlwaysEncryptedEnclavesSampleCode

Microsoft

Thank you

Pieter Vanhove
Pieter.Vanhove@microsoft.com