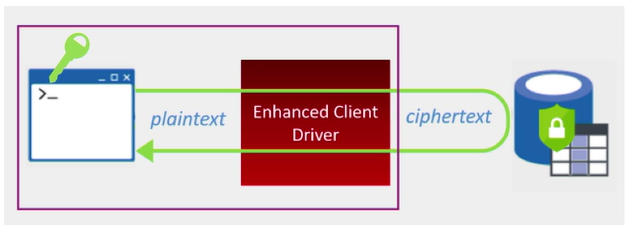
# SQL Always Encrypted

### How Always Encrypted Works

* Client-side encryption
* Driver encrypt the data, data transparently encrypted inside a client driver
* SQL server doesn’t see the plain text
* Key is stored out of SQL server, client manage the encryption keys
* Key can be stored in different stores
* Two methods to encrypt
  + Randomized encryption, much secure but prevent to do any operation on data
  + Deterministic encryption, produce same value for given plaintext, allows grouping, filtering by equality and joining tables based on encrypted values
    - Equality joins
    - Exact match searches
    - Group by operations
* Azure Key value can be used to store keys



### Controlling Performance Impact of Always Encrypted

Because Always Encrypted is a client-side encryption technology, most of performance overheads are observed on the client side, not in the database. Apart from the cost of encryption and decryption operations, the other sources of performance overheads on the client side are:

* Additional round trips to the database to retrieve metadata for query parameters.
* Calls to a column master key store to access a column master key.

### Resources:

* [Always Encrypted (DB engine)](https://msdn.microsoft.com/en-us/library/mt163865.aspx)
* [Configure Always Encrypted using SSMS](https://msdn.microsoft.com/en-us/library/mt757096.aspx)
* [Extensible Key Management Using Azure Key Vault (SQL Server)](https://msdn.microsoft.com/en-us/library/dn198405.aspx)
* [Develop Applications using Always Encrypted with the .NET Framework Data Provider for SQL Server](https://msdn.microsoft.com/en-us/library/mt757097.aspx#Anchor_4)

##### Code Samples

* [Using Azure Key Vault Key Store Provider for Always Encrypted](https://blogs.msdn.microsoft.com/sqlsecurity/2015/11/10/using-the-azure-key-vault-key-store-provider-for-always-encrypted/)
* [Provisioning Always Encrypted – Thuru’s Blog](https://thuru.net/2016/03/03/provisioning-always-encrypted-in-sql-databases-with-azure-key-vault-using-ssms-2016/)

##### Patrick’s test and sample

* I built a fully functional POC
* Azure SQL DB, enabled for Always Encryption
* A sample C# console app to communicate with SQL DB

