**KO4 - Able to secure Azure Storage account**

Azure Storage accounts provide a wealth of security options that protect your cloud-based data.

Azure services such as Blob storage, Files share, Table storage, and Data Lake Store all build on Azure Storage.

**1.Encryption at rest**

* All data written to Azure Storage is automatically encrypted **by Storage Service Encryption (SSE)** with a **256-bit Advanced Encryption Standard (AES) cipher**, and is FIPS 140-2 compliant.
* SSE **automatically** encrypts data when writing it to Azure Storage. When you read data from Azure Storage, Azure Storage decrypts the data before returning it.

**2.Encryption in transit**

Keep your data secure by enabling transport-levelsecurity between Azure and the client. Always use **HTTPS** to secure communication over the public internet.

**Role-based access control**

* To access data in a storage account, the client makes a request over HTTP or HTTPS. Every request to a secure resource must be authorized. The service ensures that the client has the permissions required to access the data.
* Azure Storage supports Azure Active Directory and role-based access control (RBAC) for both resource management and data operations.

**Auditing access**

* Auditing is another part of controlling access.
* You can audit Azure Storage access by using the built-in Storage Analytics service.