FACTSHEET

ENCRYPTION SERVICES

Protecting Your Keys

WHAT ARE KEYS?

Data encryption is classified in two variations, symmetric and asymmetric, based on the number of keys used. In symmetric encryption, a single key is used to both encrypt and decrypt the data. As the key is shared, there is a high chance of compromise. Key rotation (changing the key periodically) reduces the vulnerability.

Asymmetric encryption uses two keys for encryption and decryption. A public key encrypts the data, while a private key is used to decrypt the data. The public key can be freely distributed since it can only encrypt data. Even if the public key is stolen it cannot be used to decrypt the data. However, the corresponding private key where the decryption occurs must be handled very securely.

Symmetric and asymmetric encryption can be used together. An organisation may encrypt bulk data with a symmetric key because its faster, and then encrypt the encryption key with the asymmetric public key of each intended recipient of the data.

"A public key encrypts the data, while a private key is used to decrypt the data."

HOW DO I PROTECT KEYS?

Key management requires careful consideration and it involves identifying who holds the keys; how they are generated and distributed; the process for rotation (i.e., creating new and retiring old keys); and how the keys are protected when stored. If the keys are not carefully handled during their lifecycle, they can be disclosed, modified, or substituted. This can lead to unauthorised access to encrypted data.

Cryptographic hardware modules are used to store keys. Hardware-based encryption offers more security than software-based encryption because it prevents key tampering or theft. For this practice, tamper-resistant security modules (TRSM) and Hardware security modules (HSM) are commonly used.

A TRSM is a hardware module installed in devices such as a payment terminal to store and generate the encryption keys and to perform encryption. A TRSM can destroy itself and render useless any data or keys stored in it if someone attempts to tamper with it.

An HSM is a hardware module used mostly in back-end systems for secure key management and decryption. It provides the ability to manage the keys according to several standards and generally are built to meet standards such as common criteria and FIPS 140. Typically, keys protected by an HSM are considered high-value keys where their compromise would cause a significant negative impact to the owner.

HSM functions include:

- **Internal secure cryptographic key generation**
- **Internal secure key storage and management**
- **Use of cryptographic and sensitive data material; and**
- **Performing cryptographic functions offloaded from application servers**
- **Vendor provided Key, Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) are three ways in which keys can be managed in the cloud.**

VENDOR PROVIDED KEYS

A key provided by a vendor for the protection of data can offer only minimal assurances as to where and how the key was generated. Was the key generated within a hardware security module or was it injected into the HSM after generation. Did it in fact use an HSM or FIPS 140-2 validated random number generator at all? Does the vendor hold the key in escrow for recovery later if required?

All these questions can call into doubt the level of trust that an organisation can have in the key that was generated by a vendor.

When using a vendor provided key you are placing complete faith in:

- **the process used to generate the key**
- **the vendor not being able to access the key; or**
- **the vendor not having a copy of the key they can use for accessing your data.**

BYOK EXPLAINED

The BYOK feature allows client to use a key from a source other than the vendor as the encryption key. That source can be their own on-premises key generation service or a third-party service provider. Using an accredited key generation and storage device such as an HSM prevents the vendor from exporting client encryption keys and using them outside the HSM. However, it does not prevent the vendor from accessing client data. BYOK gives clients the following advantages over using keys generated by the vendor's CAs:

- **The Client knows the details of their key**
- **The Client can revoke their key and prevent anyone from decrypting data encrypted with that key.**
- **The Client has a copy of their key allowing them to more easily transition to another service provider should they wish to.**

The Bring Your Own Key process for providing a key for information stored in a cloud service provides a higher level of confidence in the quality of the process for the creation

of the key, but unless the key can be injected into an HSM without the possibility of interaction with the vendor the assurance given to the key cannot be without question.

When the key is transported to a Cloud Vendor using a Key Encryption Key (KEK) can you be sure that the KEK was created on an HSM and the Key you are providing cannot be unencrypted outside of an HSM.

When using a BYOK you are also placing a large amount if trust in the cloud vendor not being able to access your data through being able to access the key on an HSM that you do not control.

BYOE EXPLAINED

BYOE (Bring Your Own Encryption) is most commonly used to refer to HYOK but can sometimes also be confused in literature with BYOK. When used in conjunction with BYOK it is used to mean HYOK which is referred to below. It can be a little different though as well, as it can also be used to indicate that the customer is not only holding keys but also performing the encryption of the data as well. Microsoft do not directly support this definition of BYOE but there are solutions that use it, that effectively work without the assistance or knowledge of the systems that they are encrypting data for.

HYOK EXPLAINED

HYOK allows client to keep their own keys in their on-premises environment. Unlike BYOK, HYOK is a configuration where clients keep their own encryption keys, and all the encryption and decryption work is done with client's on-premises hardware.

Having the encryption held by the cloud service consumer or it's separate provider, allows correct jurisdictional controls to be reasserted. It does not prevent data from having to be provided where a valid court order or subpoena is provided.

This also means that should the consumer wish to change providers, they can ensure all data in the outgoing providers data is destroyed through the simple action of destroying the key.

CASB offerings may also enable tokenisation services, in which sensitive information is replaced with a token on storage, and is then replaced with real values on retrieval.

HYOK vs BYOK

Advantages and Disadvantages of BYOK

Advantages	Disadvantages
BYOK is more cost effective.	**Keys may not be protected in the way that the customer would want**
Works with Office 365.	**The Client is not the only one who has the key.**
DLP, transport rules and eDiscovery can be provided	**The Customer cannot control who will have access to the key**
Allows the customer to avoid vendor lock in as the customer has a copy of the key that they can use to unlock their data.	**The Customer does not have control over who will have access to their data 1.**
	Information is not protected from the vendor holding the data.
	Jurisdictional overreach is still possible under this model (i.e. a foreign Government court or intelligence agency could request access to the information where the company has a footprint in that country).

[1] Response to GCIO Cloud Computing Information Security & Privacy Considerations: https://gallery.technet.microsoft.com/Response-to-GCIO-Cloud-e117bbb9

HYOK vs BYOK

Advantages and Disadvantages of HYOK

Advantages	Disadvantages
HYOK works on Office 365 for instance. Microsoft has even introduced their own version of it.	**Added security comes at a cost.**
The Client knows no one has access to their data without their approval. They hold the keys.	**Clients have to maintain their own on-premises encryption infrastructure. If something goes wrong, the client could be locked out of their own data.**
Allows the customer to avoid vendor lock in as the customer has a copy of the key that they can use to unlock their data.	**Any data encrypted with HYOK cannot be accessed by ANY Office 365 services.**
Can allow a customer more choice on who is doing the encryption	**It is more difficult (but not impossible) to provide a client with services such as DLP, transport rules and eDiscovery.**
Allows the customer to have a greater level of assurance that the service provider and their staff cannot get access to their data.	**Some vendors, Microsoft for instance, claim that none of the advanced data handling features of Office 365 will work and this is certainly true of their solution but not of all other solutions.**
Avoids jurisdictional overreach. HYOK means that the laws of the customer, not the provider, are enacted to access data.	**Setting up HYOK does require considerable configuration**