DATASHEET

Key Management as a Service

Securely store important keys for on-premise and cloud based services
Strong key control and security

KNOW YOUR KEYS ARE SECURE

Key Management as a Service (KMaaS) is a Cogito service that allows customers to securely store important keys for on premises and cloud-based services that they consume.

The KMaaS can also be used to:

- **protect keys for Public Key Infrastructure (PKI) capability**
- **to allow for encrypted storage in the cloud or on premises**
- **Transparent Data Encryption (TDE) on Databases on premises or in cloud instances**

It can be used for:

- **Bring Your Own Key (BYOK) and**
- **Hold Your Own Key (HYOK)**

BYOK is where a key is generated on a HSMs to ensure that it has a good Radom Number Generator used in it's generation. A copy is kept for archival on that HSM as well as a copy being given to the service provider.

HYOK is where a key is generated on our HSMs to ensure that it has a good Radom Number Generator used in its generation. This copy is then leveraged by on premises and cloud services to provide the required encryption capability. A copy is also securely archived, but a copy is not given to the service provider as it is in BYOK.

Benefits include:

- ✓ **Strong Key Control and Security**
- ✓ **Cost reduction - reduce the cost of hosting specialised key management services;**
- ✓ **Expertise and Compliance to best practise policies**
- ✓ **Minimise risk and ensure your keys don't leave a region or legal jurisdiction;**
- ✓ **Enhanced Capability from wholistic key management**
- ✓ **Easy to transition out and avoid vendor lock in**

“If the keys are not carefully handled during their life cycle, they can be disclosed, modified, or substituted. This can lead to unauthorised access to the encrypted data.”

“Tamper resistant security module (TRSM) and Hardware security module (HSM) are commonly used to protect keys”

What are keys?

Data encryption is classified into two types:

1. symmetric and

2. asymmetric.

Symmetric encryption uses a single key. In symmetric encryption, a single key is used to both encrypt and decrypt the data. As the key is shared, there is high chance of compromise. Key rotation (changing the key periodically) reduces the vulnerability.

Asymmetric encryption uses two separate 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.

Typically, keys protected by a HSM are considered *high-value* where their compromise would cause a significant negative impact to the owner.

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 (creating new and retiring old keys); and
- how the keys are protected when stored.

If the keys are not carefully handled during their life cycle, they can be disclosed, modified, or substituted. This can lead to unauthorized access to the 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.

"Cogito has a vast amount of experience with key management and protection in a number of forms such as storage in HSMs.

Cogito has sold and supported HSMs since its inception. It has staff however that have been supporting HSMs for much longer.

Cogito has many decades worth of experience with a number of products including the following:

- ✓ Safenet/Gemalto/Thales Luna, Key Secure and Vormetric product lines;
- ✓ nCipher (formally Thales eSecurity) Connect, Solo and Edge series;
- ✓ Fortanix
- ✓ Cavium
- ✓ Ultra (formerly AEP)
- ✓ Utimaco
- ✓ Blackbox "

HSMs and TRSMs

Tamper resistant security module (TRSM) and Hardware security module (HSM) are commonly used to protect keys.

A TRSM is a hardware module that is 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.

A 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 a 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**

How are keys managed in the Cloud?

There are three ways keys can be managed in the cloud:

1. **Vendor provided Key,**
2. **Bring Your Own Key (BYOK) and**
3. **Hold Your Own Key (HYOK**

Cogito Group is an award-winning ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies.