Fact Sheet

Cogito Group

Key Management as a Service

Know Your Keys Are Secure

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

KMaaS provides strong key control and security that can be used for the following:

- Protecting keys for Public Key Infrastructure (PKI) capability.
- Allowing encrypted storage in the cloud or on premises.
- Transparent Data Encryption (TDE) on Databases on premises or in cloud instances.
- Generating and managing API keys.
- Bring Your Own Key (BYOK).
- Hold Your Own Key (HYOK).

Types of Keys and Key Material that can be Generated

There are many types of keys and key material that can be generated using the Cogito Service. This includes:

- API keys
- Symmetric keys such as AES and 3DES
- Asymmetric keys such as RSA and ECC keys
- CSRs

Benefits of KMaaS

There are many benefits to the Cogito KMaaS. Some of these are:

- Strong key control and security.
- Ability to recover keys from archive for reuse on new or existing services
- 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.
- Allows easy transition out of a service as it avoids vendor lock in.

What are Keys?

Data encryption is classified into two types:

Symmetric Key Encryption

Symmetric key encryption uses a single key. In symmetric key 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, such as changing the key periodically, reduces the vulnerability.

Asymmetric Key Encryption

Asymmetric key encryption uses two distinct and 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 and even if the public key is stolen it cannot be used to decrypt the data. The corresponding private key, however, must be handled very securely as it is used in decrypting the data.

Symmetric and asymmetric key 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.

How do I Protect Keys?

Key management requires careful consideration and involves identifying:

- Who holds the keys.
- How they are generated and distributed.
- The process for rotation (creating new and retiring old keys).
- 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 as it prevents key tampering or theft.

How Are Keys Managed in the Cloud?

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

- Vendor generated/provided Keys.
- Bring Your Own Key (BYOK).
- Hold Your Own Key (HYOK).

Vendor generated/provided Keys

Vender generated keys are where you generate and store keys using the vendors inbuilt services. Often these services, even including providers such as Microsoft and Amazon have lower standards than some organisations would accept for services they would run internally despite the greater risk presented by internet accessible services. An example is both vendors use FIPS140-2 Level 'validated' HSMs and state this on their websites. This is true. The hardware they use has been validated to FIPS140-2 Level 3 standard, however both vendors actually operate the HSMs in the lower FIPS140-2 Level 2 mode. Cogito provides a service that operates at FIPS140-2 Level 3 mode. The other important factor with vendor provided services is that keys generated in these services often cannot be exported or recovered. This results in being locked to a particular vendor for a service once data is better protected using encryption.

Bring Your Own Key (BYOK)

BYOK is where a key is generated on an HSM to ensure that sufficient Random Number Generator used in the key's creation. A copy of the key is kept for archival purposes on the Hardware Security Module (HSM) and a copy is provided to a service such as AWS or Azure. This allows for keys to be recovered reducing vendor lock in. That includes the BYOK service run by Cogito itself. A customer can leave the service at any time and take all key material with them when they do leave.

Hold Your Own Key (HYOK)

HYOK is where a key is generated on our HSM to ensure that sufficient Random Number Generator used in the key's creation. This key 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.

HSMs and TRSMs

A Tamper Resistant Security Module (TRSM) and a 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.

An HSM is a hardware module used mostly in back-end systems for secure key management and decryption. It provides the ability to manage keys according to several standards and 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.
- Performing cryptographic functions offloaded from application servers.

Key Management as a Service

Fact Sheet

HSM Experience

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

- 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.

Cloud Integrations

Bring Your Own Key (BYOK)

BYOK is **an encryption key management system that allows enterprises to encrypt their data and retain control and management of their encryption keys.** Keys can be generated in Cogito HSMs through the Jellyfish interface, and these can be wrapped and exported securely to be imported into a Cloud Provider for use in cloud computing.

Supported platforms include:

- **Amazon Web Services** KMS (Key Management Service)
- **Azure** Key Vault
- **Google** Cloud Platform CSEK (Customer-supplied encryption keys)
- **Salesforce** Shield Platform Encryption

Credential Sync

When issuing Certificates through the Jellyfish interface, the Certificate and Private Key can be automatically pushed to your Cloud instance with a single click.

Supported platforms include:

- AWS Certificate Manager (ACM)
- Azure Key Vault

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated 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. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.