Fact Sheet

Cogito Group

Enterprise Key Management Overview

Key Management

Cogito Group provide a variety of Key Management Services to customers through the Cogito Group Security Services Environment. These services support customers by ensuring that keys are generated, stored, and managed in a professional, purpose-built environment to provide assurance that the information protected by Cogito Group managed keys retains confidentiality, integrity and availability throughout the information lifecycle.

The Cogito Group Key Management Services are provisioned with both security and availability in mind. All keys are stored in FIPS 140-2 Level 3 Hardware Security Modules, which may be either part of online systems (where keys are expected to be used frequently), or as part of offline dedicated key storage environments, to be used for long-life infrequently used keys.

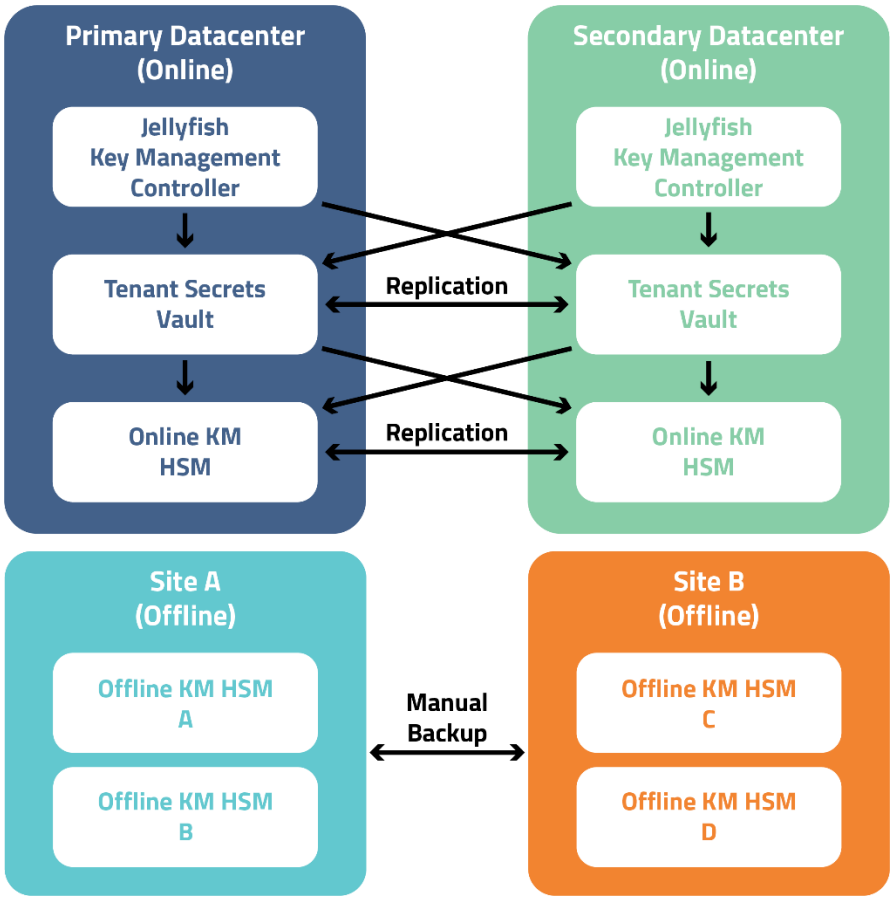

Figure 1 - Key Management Service Environment

Enterprise Key Management Overview

Fact Sheet

Cogito Group provide management over keys and other secrets either through the Jellyfish Key Management Controller – a web application with a full featured API for integration activities, or directly through the hardware security module where an on-premise solution requires it. The most secure offline keys are only ever managed in Key Management Ceremonies with suitable representatives from the customer's organisation present.

While Cogito Group primarily provide these services through Cogito Group Security Services private cloud environments, we are also able to deliver the same functionality in an on-premise, managed solution with ongoing support and maintenance where required.

Use Cases

Bring Your Own Key (BYOK)

Many cloud services now support Bring Your Own Key capabilities, which allow for tenants to provide encryption keys that are stored in cloud HSMs. Cogito Group Key Management Services provide a secure means for customers to generate strong encryption keys and deliver those keys to cloud services such as Azure, AWS, and Salesforce.

Keys are generated in a Key Generation Ceremony on dedicated, offline FIPS 140-2 Level 3 hardware, and are then prepared for export to the cloud service. The generated keys are then backed up across several failure-independent storage devices which are spread across multiple geographically diverse locations. Customers can request access to the generated keys at any time.

Cogito Group protect and manage customer keys in accordance with the Cogito Group Key Management plan, which has been designed to support high security service environments and is implemented with trained and suitably cleared staff.

TLS Offload

TLS (SSL) is fundamental to modern communications security and provides confidentiality, integrity, and non-repudiation between parties communicating over a network. Cogito Group's TLS Offload capability allows for organisations to scale their web-facing applications without compromising performance and ensuring that the server authentication keys are stored securely in a managed FIPS 140-2 L3 Hardware Security Module, protected with dedicated hardware tokens.

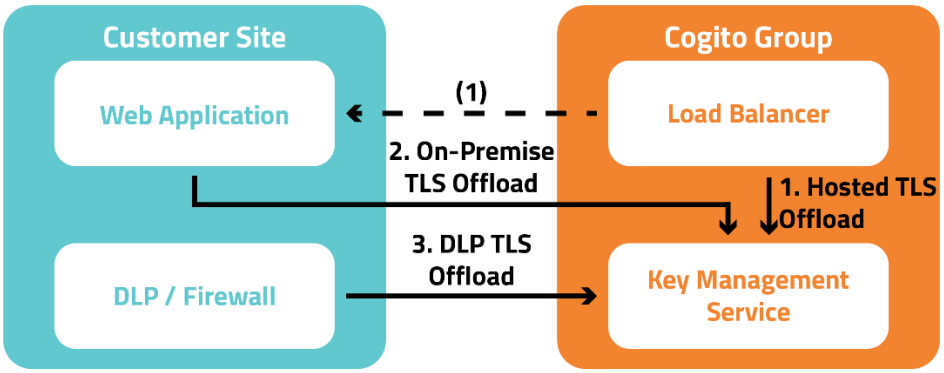

Figure 2 - TLS Offload Use Cases

The TLS Offload capability can also be used to support Data Loss Prevention and Intrusion Detection Systems hosted on-premise at a customer site to provide additional security to the high-risk key material that is required for the functionality of these services.

Cogito Group can provide TLS offload either proxied through a Cogito Group hosted load balancer or can provide access to Hardware Security Modules over a VPN connection to the Cogito Group service environment.

Digital Signature and Encryption Services

With a strong background in PKI and authentication solutions, Cogito Group provide a number of digital signature services, with modern API integration options alongside intuitive user interfaces for end users. All signing keys are protected securely in the Key Management Environment. Cogito Group have a number of options for segregation of trusted keys to fit all customer requirements.

Cogito Group currently support the following digital signature and encryption services:

- Microsoft Executable and DLL Signing.
- Microsoft Macro Signing.
- Document Signing.
- Trusted Timestamping.
- DNSSEC.
- Secure Email Services (including, but not limited to S/MIME).
- Email Gateway Encryption.
- EMRTD Signing.
- Office365 Cloud Encryption.
- JWT Signing.

In addition to application of digital signatures, Cogito Group offers validation services for all signature services. Custom solutions for specific use cases are also available to fit most use-cases.

Database Encryption

Encryption of data at rest is an effective security control to reduce the impact of unauthorised data access by malicious third parties. The Cogito Group Key Management Service can be used to directly integrate with a number of database solutions such as Oracle, MS SQL, PostgreSQL, and MySQL. Encryption keys can be generated in Cogito Group Key Management Services where they may be managed through the Jellyfish Key Management Interface or exported for use in cloud databases.

Secret Management

Enterprises now have a strong reliance on IT services, which often comprise large numbers of secrets such as service account credentials, API keys, and other encryption keys. Cogito Group Key Management Services provide a full secrets vault capability to provide easy and secure management of keys.

All keys are stored in an encrypted database with strong tenancy separation controls and role-based access control functionality to ensure that only correctly permissioned users may access the secrets. The secret management service provides a REST API to enable programmatic access to the keys inside, meaning that keys may be pulled as required rather than stored in plain text in configuration files.

The Secret Management service has been designed with enterprise applications in mind, providing support for privileged access management, identity access management, and card management solutions, as well as automation and bespoke applications.

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.