



## KEY LIFECYCLE MANAGEMENT

### Why Key Management?

Technology trends point towards greater systems connectivity, larger data volumes and higher electronic transaction values. To secure these increasingly complex systems requires the management of ever larger numbers of cryptographic keys – from the tens towards the thousands, for medium to large organisations. Increasingly, such organisations, in particular in the financial sector, deploy secure key management systems dedicated to this task.

In addition to rising volumes of cryptographic keys, many financial institutions are facing an increasing regulatory burden imposed by credit and debit-card payment schemes and the Payment Card Industry (PCI) standards. Information security, and thus key management, is central to compliance.

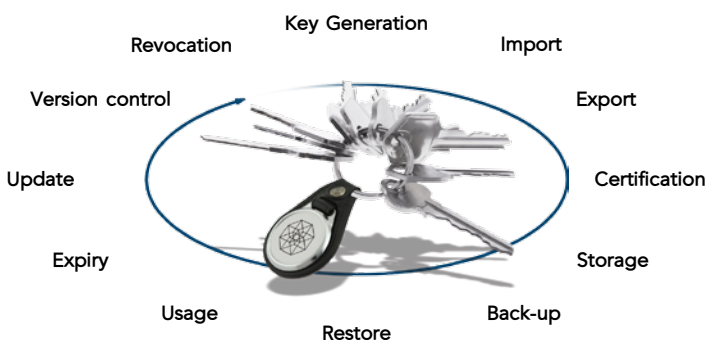
### What Is Key Management?

To many people, key management is the generation and exchange of cryptographic keys. However, *end-to-end lifecycle* key management includes generation, distribution, usage, expiry, revocation and update of keys. It's about having the right key, in the right place, at the right time.

Traditionally, key management has been managed through inefficient paper-based procedures and multi-party key 'ceremonies'. Achieving high security in this manner can be extremely resource intensive, with at least 3-4 staff members involved in each instance. In many cases today, organisations are left with no central surveillance of their keys, their location, their use, when they expire, or who is responsible for them. Those organisations are faced with enormous increases in workload and costs.

### Cryptomathic Key Management System

Cryptomathic KMS uses a client-server based architecture, with shared HSMs, to provide a centralised key management solution. The system is accessed by operators using desktop computers equipped with secure PIN pads for key component entry. An extremely flexible 'key-push' protocol allows the Cryptomathic KMS server to securely connect with practically any secure host system that supports exchange of cryptographic keys.



Both symmetric keys and asymmetric key pairs (and their corresponding certificates) are easily managed using Cryptomathic KMS Key Projects. A Key Project represents the current state of a set of keys as well as their history and general lifecycle management. Working with Key Projects enables efficient operation through the possibility to automate and optimise the working processes while adhering to the strictest set of security standards.

Needless to say, full compliance with all relevant industry and government regulations and best business practice is maintained throughout, with the added benefit of automated key management across multiple sub-systems and a central view of all cryptographic keys within the business as a whole.

### Cryptomathic KMS Benefits

- Consolidated Management – security officers can set up projects to manage logical sets of keys as a single entity. It also allows for other security officers to review and execute projects once complete.
- Reduced Dependency – asynchronous log-on to projects allows for key custodians to add components securely as they are available, reducing the need for key ceremonies.
- Mobility – allows security officers and custodians to manage keys over a network. Operators no longer need to be monitored using physical room security mechanisms such as video surveillance, physical room access control and hard-copy-logging, due to the Cryptomathic KMS desktop terminals which have hardware security mechanisms, smart-card access and local printing of key components.
- Centralised – securely manage keys across multiple parties/zones, i.e. banks, personalization bureaus, payment schemes, etc.
- Automated – securely push keys to any key distribution target as and when required.
- Lifecycle Management – each project maintains its own audit logs allowing for complete accountability and returning to a given state at any point in time of the project.

## TECHNICAL SPECIFICATIONS

### System Architecture

- Multiple or single servers
- Multiple or single HSMs
- Simple integration and automated production through a dedicated API
- Flexible integration with existing cryptographic sub-systems

### Keys

- Multiple algorithms (DES, AES, RSA, etc.)
- Multiple key types (Master Key, Zone Key, Key Encryption Key, etc.)
- Support for groups of keys (EMV key sets, etc.)

### Security Architecture

- AES protected network communication
- Access control via smart cards
- Secure environment using HSMs
- HSM programming for key and certificate management
- Secure audit log of all events (in HSM)
- Secure PIN pad for secure key custodian work

### Secret Sharing Schemes

- Key shares on chip cards
- Key shares on PINpad
- Key shares on file
- XOR key shares

### Protocols

- SOAP
- Web service used for handling asynchronous targets

### Syntax, Certificate Formats and Requests

- X.509v3, PKCS#10
- EMV
- DES, 3DES, RSA (PKCS#1, PKCS#8), AES, SHA-1

### Operating Environment

- Microsoft Windows

### Database

- Microsoft SQL Server
- Oracle

### Hardware Security Modules

- IBM
- Thales / nCipher
- SafeNet
- Other HSMs upon request

### Key Targets

- Any HSM or security terminal\*

\* Please contact Cryptomathic for the latest status.

## MANAGEMENT OF KEY LIFECYCLES USING CRYPTOMATHIC KMS KEY PROJECTS

The concept of working with Key Projects is central to using Cryptomathic KMS. It allows an organisation to enforce its procedures related to its various staff groups, e.g. key custodians, security officers and even security auditors if required, and lets each group perform their task – while no other person or group is left idle.

Keys can be generated, installed, backed up, restored, disabled, re-enabled, updated or – at the end of life – deleted. A central view allows for an easy overview of keys and their status. Additionally, interactive flags and reminders let the system operators know that action may be required in the near future e.g. related to key- or certificates updates. Keys and any information related thereto (version control, certificates, etc.) are managed in such a way that reports on all key-related events throughout the systems history may be viewed at a later stage if required.

Additionally, the dynamic definition and set-up of key types and targets in Cryptomathic KMS allows for organisations to set up secure communication with practically any system.

### Key Advantages

Streamline processes

Avoid human error

Cost saving – eliminate custodians

Fewer HSMs

Centrally managed upgrades

## ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With more than 20 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing

and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at [cryptomathic.com](http://cryptomathic.com)