



CRYPTOMATHIC KEY MANAGEMENT SYSTEM (CKMS)

Why Key Management?

Technology trends point towards greater systems connectivity, larger data volumes and higher electronic transaction values. To secure the 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 key materials, many institutions are facing an increasing regulatory burden. As well as conforming with major credit- and debit-card payment schemes and Payment Card Industry (PCI) standards, information security, and thus key management, are central to compliance.

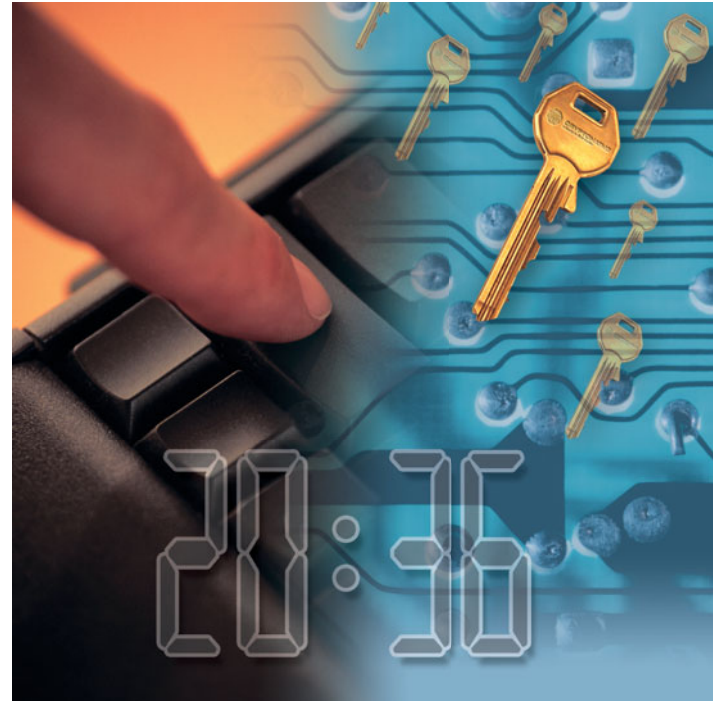
What Is Key Management?

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

For some time, key management has been managed through inefficient, paper-based key management procedures and multi-party key 'ceremonies'. Achieving high security in this manner is extremely resource-intensive. As a result, most organisations today have no central view of their keys, their location, their use, when they expire, or who is responsible for them. Those organisations that do are faced with enormous increases in workload and costs.

Of course, this is achieved with the strongest technical and procedural security controls and in full compliance with all relevant industry and government regulations, and best business practises.

CKMS uses a client-server architecture, with a hardware-enhanced server, accessed by operators using desktop computers equipped with secure PIN pads for key component entry. An extremely flexible key-push pro-

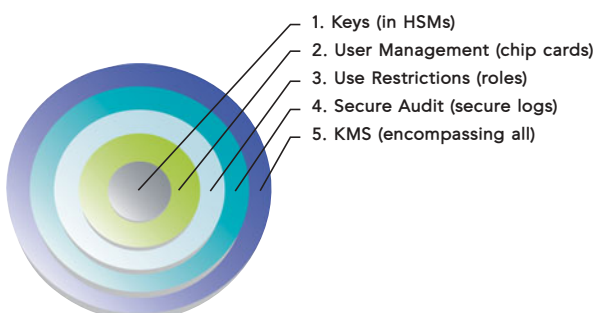


ocol allows the CKMS server to securely connect with practically any secure host system that supports exchange of cryptographic keys.

Both symmetric keys and asymmetric key pairs (and their corresponding certificates) are easily managed using CKMS Key Projects. Working with Key Projects enables efficient operation through the possibility of optimizing the working processes while adhering to the strictest set of security standards.

CKMS:

- Key Projects – work smart and securely allowing security officers to set up projects and enable key custodians to perform their duties. It also allows for other security officers to review and execute a project once complete.
- Work smarter (not harder) – asynchronous log-on to projects allows for extremely flexible workflow management and minimise time spent on performing simple tasks.
- Mobility through security – allow security officers and custodians, to manage keys over a network. In effect, CKMS 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 CKMS desktop hardware security mechanisms.
- Securely manage keys across zones (between different parties, i.e. banks, personalization bureaus, payment schemes, etc.)
- Securely push keys to any key distribution target.
- Manage key life cycles – each project maintains its own log allowing for complete audit logs and returning to a given state at any point in time of the project.



TECHNICAL SPECIFICATIONS

System Architecture

- Multiple servers
- Multiple HSMs
- System integration API for automated production
- Flexible Key Target Set-up

System Keys

- Master Keys (MK)
- XOR key shares
- Zone Master Keys (ZMK)
- Key Encryption Keys (KEK)

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

Cryptographic Formats

- DES, 3-DES
- RSA Algorithm (PKCS#1)
- SHA-1

Secret Sharing Schemes

- Key shares on chip cards
- Key shares on PIN pad
- Key shares on file

Protocols

- SOAP
- Web service used for handling asynchronous targets

Syntax, Certificate Formats and Requests

- X.509v3, PKCS#10
- EMV

Operating Environment

- Microsoft Windows: 2003 Server
- Client: Windows XP

Database

- Microsoft SQL Server 2005

Hardware Security Modules

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

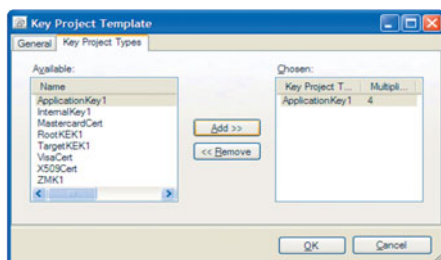
Key Targets

- Any HSM or security terminal*

*Note: Please contact Cryptomathic for the latest status.

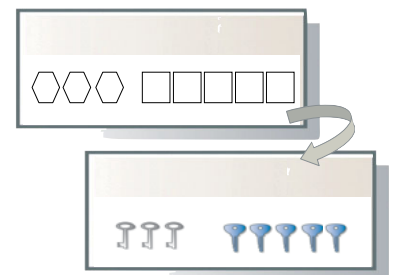
MANAGEMENT OF KEY LIFE CYCLES USING CKMS KEY PROJECTS

The concept of working with Key Projects is central to using CKMS. It allows an organisation to enforce its procedures related to its various staff groups (i.e. IT staff, key custodian staff, security officers and even security auditors if required) and let 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. An easy-to-use traffic light system 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 CKMS allows for organisations to set up secure communication with practically any system.



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 20 years' experience, we have assisted our customers by providing systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing, and advanced key management through best-of-breed security software and services.

Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with its 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