CRYPTOMATHIC

Crypto Key Management System

Product Sheet

CKMS

Ultimate control and visibility of your cryptographic keys

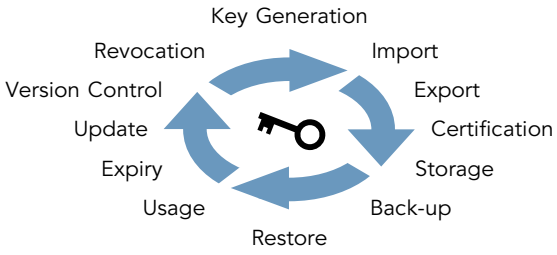
CRYPTOMATHIC

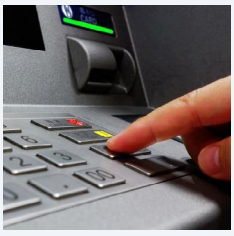
Take control and achieve compliance with centralized and automated application key management

Cryptographic keys underpin the protection and reputation of your business. But managing an increasing number of keys is challenging; manual processes are costly and error prone; demonstrating compliance is time-consuming.

CKMS delivers efficient, centralized and automated key management to a broad range of applications, ensuring the appropriate keys are available at the right time and place. CKMS supports robust business processes and allows you to confidently comply with and pass internal / external audits.

- Centrally manages the life cycle of cryptographic keys at large scale
- Automates key management activities and on-line key distribution
- Reduces the risk of key compromise and human errors
- Provides tamper evident audit and usage logs for compliance
- Streamlines key management processes and reduces costs



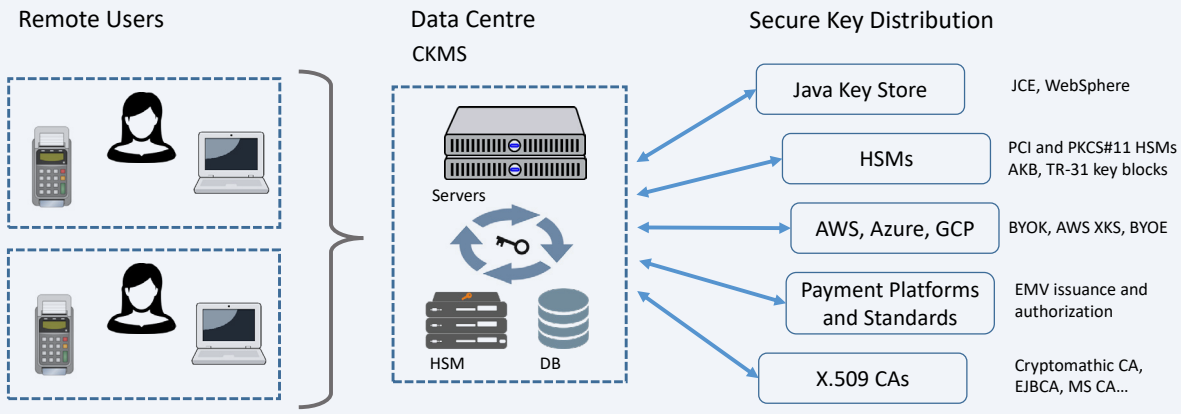


Typical Use Cases

CKMS is trusted around the world to manage:

- Payment keys for card issuance and authorization
- PCI DSS, PCI Key blocks, PCI PTS compliance
- ATM and POS remote key loading (RKL)
- HSM application keys, integration to e.g. Atalla, Thales HSMs, etc.
- Cloud key management, BYOK and BYOE to AWS, Azure, GCP
- AWS XKS
- Data protection and data sovereignty in multiple jurisdictions (GDPR, SHREMS II, SOC…)

Crypto Key Management System



Technical Architecture

CKMS is built on a resilient client-server architecture. Hardware Security Modules (HSMs) are used to ensure high-quality key material and strong protection of encrypted keys held in an external database. High availability is ensured through clustering of the server, database and HSMs. Key management administration can be performed without restrictions on time and place via an intuitive GUI or automated using REST APIs. Key Loading Devices supports remote manual key component management like key import/export via TR-31 format and key share printing. Keys are distributed to applications and HSMs in a wide range of formats. All critical operations are recorded in a tamper-evident audit log.

Security / Certification / Features

- Use of FIPS 140-2 level 3 HSMs
- PCI Key Loading Device, PCI HSM v3 compliant
- PCI-DSS - Key Management Requirements
- PCI-HSM - Security Requirements
- PCI Key Blocks Requirements

Technical Specifications

Operating System:

- Windows Server

DB:

- MS SQL
- Oracle
- Maria DB

HSMs:

- Entrust
- Thales
- Utimaco

Key Block Formats:

- Atalla Key Block
- IBM CCA
- PKCS#8 Cryptogram
- TR-31

Key Types:

- Algorithms: AES, DES, 3DES, ECC, RSA
- Keys & certs: CVK, EMV, PGP, PVK, SSH, ZMK, ZMKP, X.509 and custom certificates

CKMS: More than just managing keys

The Crypto Key Management System (CKMS) was first deployed at a customer in 1998 to centrally manage keys throughout its entire payment network. CKMS is now used by major organizations and financial services companies worldwide to centrally control and automate the life cycle of millions of keys. Combining CKMS with CSG offers a complete infrastructure for total control of all crypto and policy functions for any application.

CKMS Case Study - Swedbank

Centralized key management for a major acquirer

Being one of the largest acquirers in Europe and managing keys for hundreds of applications, Swedbank has modernized its cryptographic key management activities to securely control the keys for its card payment acquirer network and its payment terminals.

CSG Case Study - Barclays

Cryptography as a service

Crypto Service Gateway (CSG) revolutionizes the management of cryptography for businesses. With CSG, Barclays now has over 125 applications running on a single crypto-agile platform, achieving significant and steadily increasing cost savings and usage growth. Providing a cryptographic business service, agile to changing business needs, CSG's philosophy is truly unique, as it offers user-friendly, transparent, vendor agnostic cryptography as a service.

ABOUT CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Identities & Signing, Payments, Mobile App Security and Crypto & Key Management through best-of-breed security solutions and services.

We pride ourselves on strong technical expertise and unique market knowledge, with two-thirds of employees working in R&D, including an international team of security experts and a number of world-renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.

Learn more at cryptomathic.com