cpl.thalesgroup.com

THALES

Centralized & Automated Key Management for payShield HSMs

The Problem:

Banks and Financial Institutions use cryptography pervasively to protect data, communications and processes. In a hierarchy of value, there will be keys critical to the core functioning of a bank – typically associated with card payment schemes (issuing and acquiring) and ATM and POS networks. These are the "keys to the kingdom". Theft or misuse of these keys would be catastrophic. However, modern IT practice means that these keys need to be made available to applications and processes both inside and outside the bank.

The Challenge: Managing the "Keys to the Kingdom"

Managing an increasing number of cryptographic keys across business applications is becoming ever more challenging. Manual, decentralized processes are costly and error prone, and demonstrating compliance is time consuming. The top three challenges of key management are frequently cited as lack of clear ownership of processes, lack of skilled personnel, and the existence of isolated and fragmented systems. Additionally, demonstrating compliance with data protection standards such as PCI DSS is non-negotiable for many enterprises.

To address these challenges and to assert strong control over the creation and distribution of the keys, a solution must enforce specific roles and set clear responsibilities over keys, while freeing staff from mechanical, repetitive tasks to orchestrate keys across disparate systems supporting standard key formats.

CRYPTOMATHIC

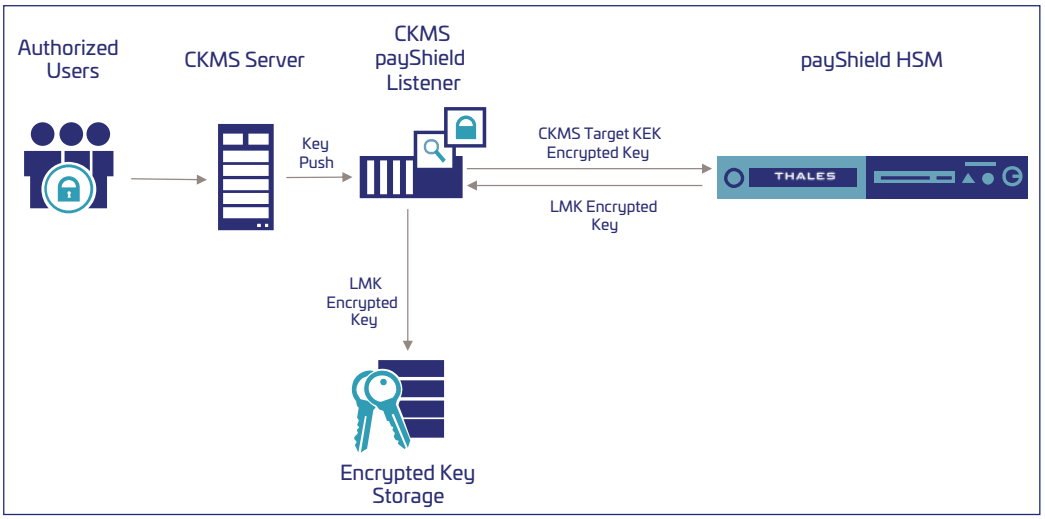
The Solution: Crypto Key Management System (CKMS) – Take control with centralized and automated key management

As a centralized key management system, the Cryptomathic CKMS directly addresses all of the above challenges, and delivers automated key updates and distribution to a broad range of applications. CKMS manages the entire lifecycle of all keys (symmetric and asymmetric), supports robust business processes and allows you to confidently comply with and pass internal and external audits.

Key Benefits

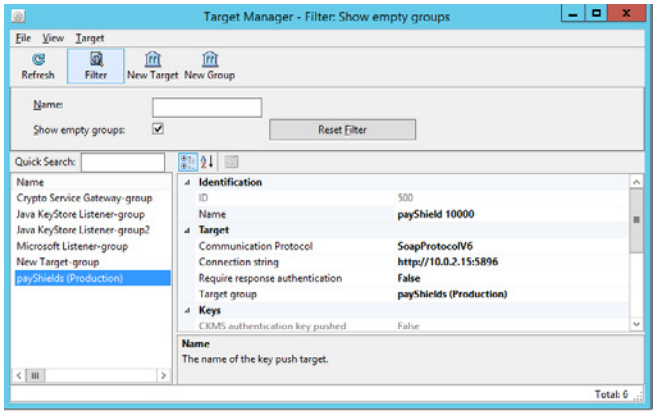
- Complete remote administration workflow, including key approval and distribution
- Central management of keys through their complete lifecycle
- Automated delivery and update of keys
- Keys shared between HSMs and applications
- Comprehensive audit logs of CKMS configuration, operation, and key management workflow

CKMS with payShield Architecture



Key management administration can be performed without restrictions on time or place via an intuitive GUI, supported by secure PIN entry devices (PEDs) and smart cards for strong authentication. The PEDs also support key import/export and key share printing. Keys are distributed to Thales payShield HSMs for immediate use by calling applications. All critical operations are recorded in a tamper-evident audit log.

With the addition of the Thales payShield HSM, CKMS's value is enhanced as the same key(s) can be delivered to a payShield HSM and a supporting business application, internal or external to the bank. CKMS supports a wide range of import and export options including key-blocks (TR-31) and supports both manual and programmatic delivery of keys.



CKMS GUI

Why use Thales payShield with Partner Product CKMS?

The Thales payShield HSM is the market leading payment HSM. The Cryptomathic CKMS is a key management system designed for the rigorous demands of banks and financial institutions. The integration combines best-of-breed products to offer an integrated solution for key-management and key-use.

Support is included for the following:

- KEK Exchange: supports KEK generated by CKMS or payShield
- Automatic generation of LMK encrypted Application Key(s)
- Application Key Support types:
  - DES3-K2
  - DES3-K3
  - AES-128
  - AES-192
  - AES-256

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

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 30 years of experience, we provide systems for Authentication & Signing, EMV and Crypto & Key Management through best-of-breed security solutions and services.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us