Cryptomathic and Entrust deliver centralized and automated key management

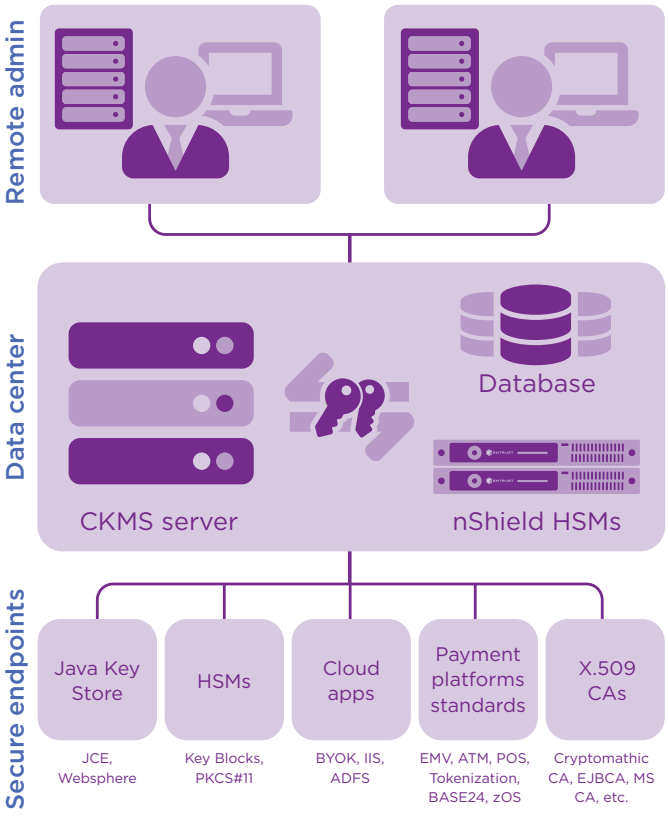
Ultimate control and visibility of your cryptographic keys throughout their life cycle – across the enterprise

HIGHLIGHTS

- Centrally manage cryptographic key life cycle at large scale
- Automate management activity and on-line key distribution
- Reduce the risk of key compromise due to human errors
- Provide tamper-evident audit and usage logs for compliance
- Streamline key management processes and reduces costs

The problem: as growing numbers of enterprise applications use cryptography, managing keys becomes a complex task

Cryptographic keys underpin the security and reputation of your business. Keeping track and managing the life cycle of increasing number of both symmetric and asymmetric keys is challenging. Manual processes are costly and error prone, and demonstrating compliance is time consuming.



Sample deployment using nShield Connect HSMs with Cryptomathic Crypto Key Management System (CKMS) Server to safeguard and manage underpinning keys. nShield® can be deployed on-premises or as a service.

LEARN MORE AT ENTRUST.COM/HSM

Cryptomathic and Entrust deliver centralized and automated key management

The challenge: effective management of keys with clear ownership across isolated and fragmented system

Safeguarding business processes from attack requires robust protection of the keys that ultimately underpin services and provide the essential roots-of-trust. Demonstrating compliance with data protection standards like PCI DSS and GDPR is non-negotiable for many enterprises.

To address this challenge, 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.

The solution: Cryptomathic CKMS and nShield Connect HSMs address key management challenges faced by the enterprise

Cryptomathic's Crypto Key Management System (CKMS) is a centralized key management system that delivers automated key updates and distribution to a broad range of applications. CKMS manages the entire lifecycle of keys (symmetric and asymmetric), including all the functions related to importing, generating, exporting, and renewing keys, as well as enforcing their correct usage. CKMS supports robust business processes and allows enterprises to confidently comply with and pass internal and external audits. CKMS is trusted around the world to manage:

- EMV keys for card issuance and authorization (e.g. BASE24)
- ATM and POS remote key loading (RKL)
- HSM application keys
- Bring your own key (BYOK) to cloud environments
- Keys for data protection (e.g., PCI DSS compliance)
- X.509 for web servers, load balancers, and more

Cryptomathic's CKMS is built on a resilient client-server architecture, integrating with nShield Connect HSMs, which ensures high quality key material and strong protection of keys and application logic. High availability is ensured through clustering of the servers, database, and HSMs.

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 applications and the nShield HSMs in a wide range of formats (key-blocks). All critical operations are recorded in a tamper-evident audit log.

Why use nShield Connect with Cryptomathic CKMS?

Keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise through theft or substitution. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield Connect HSMs integrate seamlessly with Cryptomathic's CKMS to provide comprehensive logical and physical protection of key material. The combination delivers an auditable method for enforcing security policies.

Cryptomathic and Entrust deliver centralized and automated key management

By providing a mechanism to enforce security policies and a secure tamper resistant environment, customers can:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed
- Protect critical CKMS application-logic through execution in the secure confines of the HSM, safeguarding against advanced persistent threats (APTs) as well as sophisticated insider attacks

nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nShield HSMs, you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing cryptographic keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG, nCore, and nShield Web Services Crypto API)

nShield is available in several form-factors: as an appliance, PCIe, USB, and as a service.

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

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, the company provide systems for authentication & signing, EMV, and crypto & key management through best-of-breed security solutions and services. Cryptomathic prides itself 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

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com