IBM and Entrust enable enterprise-wide encryption for data at rest

Key lifecycle management with hardware root of trust creates a security-immune enterprise system

HIGHLIGHTS

- Integrate with wide range of enterprise data encryption clients
- Use standards-based Key Management Interoperability Protocol (KMIP)
- Enable crypto key generation, submission, retrieval, and deletion
- Support on-premises, cloud, and hybrid encryption solutions
- Integrate with a FIPS and Common Criteria-certified root of trust

The problem: increasing volume of data at rest across enterprise systems at risk of compromise

Insider threats, aging, lost or stolen tape drives, and necessary storage upgrades and maintenance can all expose sensitive data at rest and compromise confidentiality and integrity. With more data being used by enterprises to conduct day-to-day business, and stricter data security regulations being enacted, data needs to be encrypted at all times.

The challenge: integrating key management functions across the enterprise end-to-end

Robust encryption offers a way to protect data at all times, even when disposing media at end-of-use scenarios. Properly managing the cryptographic keys ensures that protected data is always available when needed, and destroying the key ensures disposed data is unusable (cryptographic erasure). Orchestrating these function across growing number of enterprise encryption clients can be very demanding.

The solution: IBM secure key lifecycle management and Entrust nShield hardware security modules

IBM Key Lifecycle Management (SKLM) platform is a crypto key distribution and management software solution that uses standard KMIP to interconnect with a wide range of on-premises and cloud-based enterprise self-encrypting devices.

LEARN MORE AT ENTRUST.COM/HSM

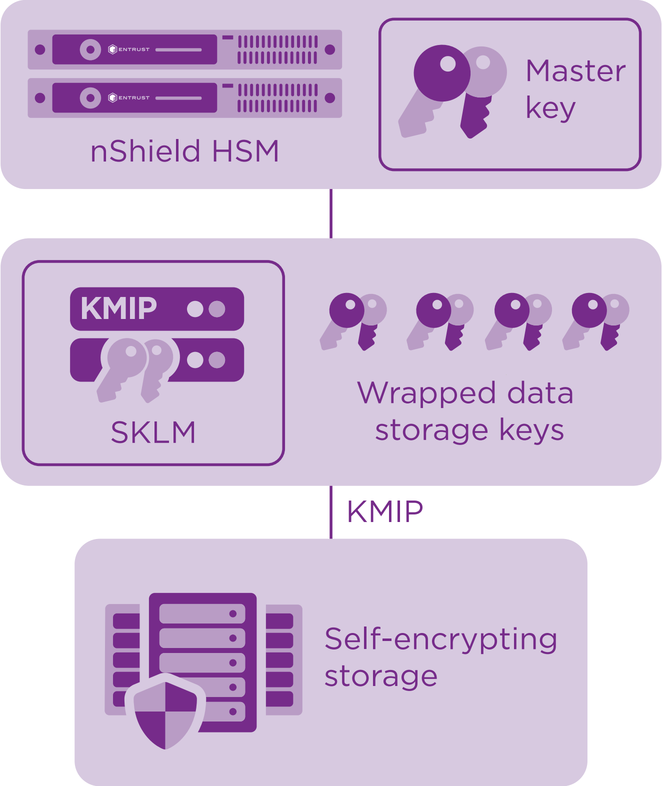
IBM and Entrust enable enterprise-wide encryption for data at rest

The solution provides centralized key generation, submission, retrieval, and deletion for data storage tape and disk arrays, and expands support for flash storage, cloud storage, and other network devices. Light-weight and highly-scalable, SKLM helps customers keep data private and compliant.

Integrating with nShield® Connect hardware security modules (HSMs), the SKLM solution ensures that master keys used to protect native keys used by the self-encrypting devices are always given the highest level of protection. Certified to FIPS 140-2 Level 3 and Common Criteria EAL4+, nShield Connect HSMs establish enforceable key use policies and a root of trust for the protection of master keys that can be deployed on-premises or as a service.

Why use Entrust nShield Connect HSMs with IBM SKLM?

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical data. The use of HSMs as a root of trust is considered a best practice by security professionals. HSMs provide a proven and auditable way to secure valuable cryptographic material. nShield Connect HSMs integrate with IBM SKLM to provide comprehensive logical and physical protection of master keys. The combination delivers an auditable method for enforcing security policies for the protection of growing enterprise data at rest. By providing a mechanism to enforce security policies and a secure tamper resistant environment for critical keys, customers can ensure the security of their sensitive enterprise data throughout its lifecycle.



Sample deployment where Entrust nShield Connect HSMs integrate with IBM SKLM platform to safeguard and manage underpinning master keys used by self-encrypting storage. nShield HSMs can be deployed on-premises or as a service.

Entrust nShield Connect HSMs enable IBM SKLM customers to:

- Secure master keys within a carefully designed crypto boundary 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 by the SKLM software
- Deliver superior performance to support demanding data retrieval production applications

IBM and Entrust enable enterprise-wide encryption for data at rest

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

With Entrust HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption 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 HSM Web Services API in conjunction with Web Services Option Pack)

Entrust nShield HSMs are 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.

IBM Security Guardium

IBM Security is a global leader in security products and services and the IBM Security Guardium offers a complete data protection suited for the diverse world of on-premises, hybrid, cloud, and multi-cloud security use cases. IBM Security Guardium is proud to be a leader in the Forrester Wave™: Data Security Portfolio Vendors, Q2 2019. See why it's a good fit for buyers seeking to centrally reduce and manage data risks across disparate database environments at **www.ibm.com/security**

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