Entrust and Cryptographic Key Management Solution Providers Simplify Enterprise Data Security and Compliance

HIGHLIGHTS

- Unify and orchestrate key management policies across your enterprise's entire infrastructure on premises, in the cloud, and in hybrid environments
- Centrally manage cryptographic key lifecycles and future-proof encryption with scalability for hundreds of millions of keys
- Support the industry API standard Key Management Interoperability Protocol (KMIP)
- Facilitate full auditing and logging for compliance with data protection regulations
- Protect your critical assets with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust

CHALLENGE

Proliferation of Cryptographic Keys

As multi-cloud data deployments become more commonplace, organizations struggle to control their critical cryptographic keys and digital security. The widespread adoption of encryption technology, driven in part by high-profile data breaches and the need for compliance, has in turn led to a proliferation of cryptographic keys used to encrypt growing volumes of sensitive data across enterprises.

Unfortunately, these keys often have no clear ownership or scalable management policy, an issue exacerbated by the scarcity of skilled personnel to manage the process. Robust digital security and compliance with government regulations and industry standards require comprehensive security policy and key lifecycle management.

Learn about our key management solutions at entrust.com

Simplifying Enterprise Data Security and Compliance

SOLUTIONS

Providing the mechanism to consistently generate and control key lifecycles at scale, Entrust and its partners offer solutions that support the KMIP standards-based approach for delivering keys to, and interacting with, client services that offer embedded cryptographic applications such as encryption. KMIP is the accepted industry standard for communicating with endpoint clients and managing key lifecycles. KMIP servers create and manage client keys, and deliver them on-demand to KMIP endpoint clients such as encrypting tape drives, storage arrays, and databases.

Entrust Key Management Solutions

Entrust's key management policy solutions provide basic or fully featured capabilities, each using the FIPS- and Common Criteria-certified Entrust nShield® Hardware Security Modules (HSMs) as its root of trust, and providing additional layers of security to administer encryption keys used by the key management servers. Available offerings include:

Entrust KeyControl

KeyControl, when integrated with Entrust nShield HSMs, supports a wide range of customers, including those who do not currently use HSMs. KeyControl's virtual appliance provides a key management server (KMS) for a large range of KMIP-compatible clients. KeyControl is VMware certified, and designed to quickly and easily deploy and scale. KeyControl is interoperable with:

- A wide range of KMIP-compliant clients, including VMware vSphere and vSAN
- Industry-standard storage arrays
- Hyperconverged infrastructure (HCI) backup platforms
- Software-as-a-service (SaaS) backup platforms

Supported endpoint application vendors include VMware, NetApp, Nutanix, and Pivot3. Support for additional endpoints coming soon.

Entrust DataControl

Integrating DataControl with Entrust nShield HSMs extends its functionality beyond just providing encryption key management. DataControl provides both KMS and encryption functionality by deploying in-guest agents called a PolicyAgent. DataControl can be leveraged for your in-guest virtual machine encryption needs across a multi-cloud, multi-hypervisor environment.

KeyControl, as the KMS component of DataControl, builds on its capabilities to extend key lifecycle management to fully managed keys providing block-level encryption to boot, root, and data drives of a virtual machine. When using the PolicyAgent of DataControl, enterprise customers can expect initial encryption and re-keying to happen with zero downtime. KeyControl, when used as part of DataControl, also offers the ability to define and enforce fine-grain access controls across hypervisors, private clouds, and public clouds such as AWS and Azure.

Technology Partner Solutions

Entrust nShield HSMs also integrate with Entrust Technology Partners' own enterprise key management solutions to deliver enhanced security with a certified root of trust.

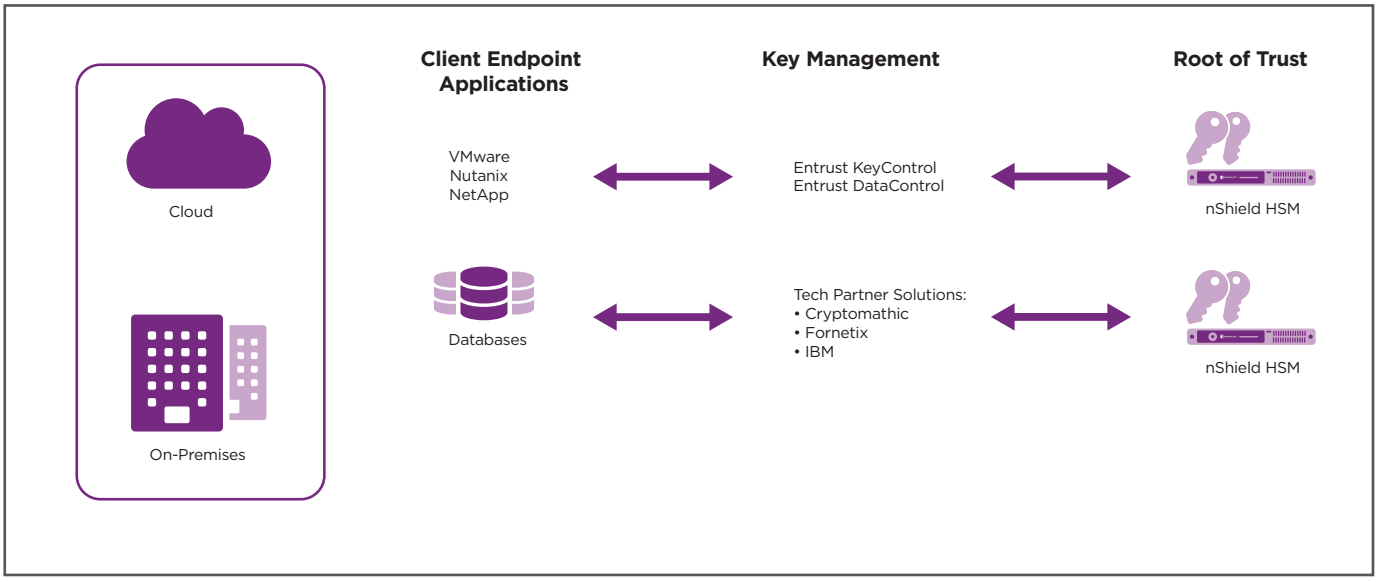
Learn about our key management solutions at entrust.com

Simplifying Enterprise Data Security and Compliance

Customers preferring a hardware-based approach over a virtual appliance, or who need to secure keys for relational database deployments, can integrate Entrust nShield HSMs with key management solutions from these technology partners.

Depending on the integration, the Entrust nShield HSM is used to provide an additional layer of security for critical keys, or to run the entire key management application within the certified boundary of the HSM. Supported technology partners include providers of cryptographic key management solutions including Cryptomathic, Fornetix, and IBM. Consult individual solution briefs for each of these specific integrations to learn more.

CRYPTOMATHIC FORNETIX IBM



Entrust nShield HSMs integrate with the KeyControl and DataControl platforms and our Technology Partners' solutions to provide an additional layer of security to enterprise key management applications.

Learn about our key management solutions at entrust.com

Simplifying Enterprise Data Security and Compliance

THE NSHIELD DIFFERENCE

Industry-Leading Technology

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They facilitate regulatory compliance and deliver 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 key access and use.

Entrust nShield Connect HSMs and nShield as a Service provide a hardened, tamper-resistant environment for performing secure cryptographic processing and key protection.

Entrust nShield HSMs:

- 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, KMIP, RESTful web services, API, and CNG)
- 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
- Deliver superior performance to support demanding security and encryption applications

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact