Venafi and Entrust deliver automated and secure cryptographic key orchestration

Integrated solution provides secure, high-speed orchestration of machine identities using certified hardware security modules (HSMs)

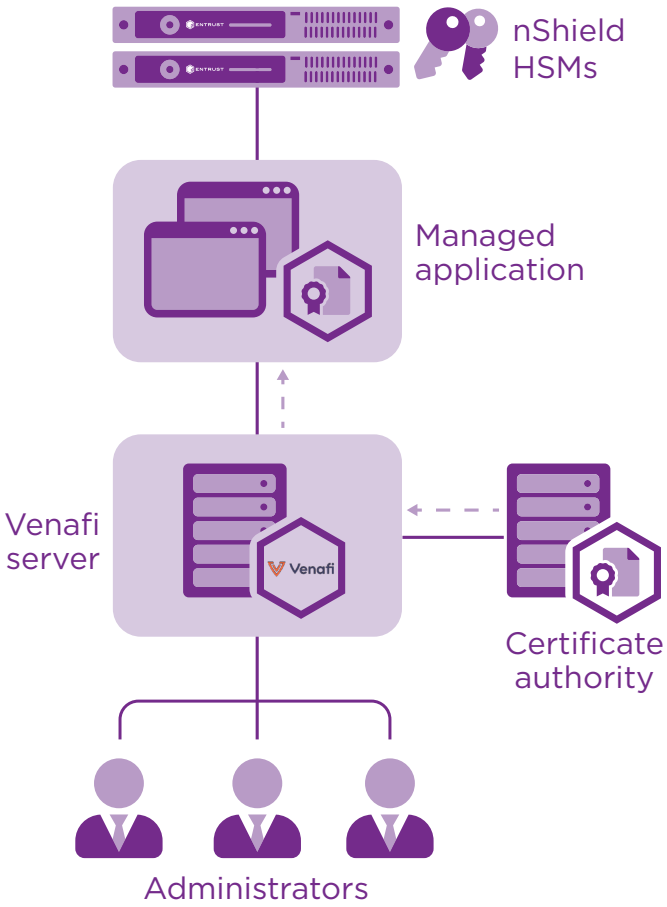
HIGHLIGHTS

- Automate lifecycle management of keys and certificates
- Protect identities of devices and applications securing critical data
- Enable trust in machines that are supporting critical business
- Apply consistent security policies to put you in complete control
- Establish a FIPS 140-2 and Common Criteria EAL 4+ root of trust

The Problem:

Identities of machines that manage critical enterprise systems and data are at risk

Organizations are increasingly dependent on machines, including devices and applications, to communicate and manage vital systems and process critical data. To discover and validate the identities of machines and protect the data they process, machine identities (digital certificates and encryption keys) are used. As an increasing number of



The Venafi Trust Protection Platform delivers key and certificate orchestration with the key pairs securely maintained by the Entrust nShield HSMs, deployed on-premises or as a service.

Learn more about our HSMs at entrust.com/HSM

Venafi and Entrust deliver automated and secure cryptographic key orchestration

attacks target signing and encryption keys, the need for strong private keys for TLS certificates, SSH, and code signing throughout the enterprise becomes more acute. Keys stored in software are susceptible to file and memory scraping, as well as side-channel attacks, both exploit information gained from system operation.

The Challenge:

Orchestrating robust hardware-based cryptographic keys at enterprise scale

Generating keys in an HSM addresses risks by producing strong FIPS-compliant signing and encryption keys with maximum entropy, using random number generation and secure hardware protection. While HSMs provide a way to secure machine identities, many organizations still opt to create custom scripts and use other manual processes to generate and provision keys, leaving them vulnerable to attack and introducing new risks to the enterprise.

The Solution:

Venafi machine identity management with Entrust nShield HSMs

Venafi and Entrust have joined forces to help address the machine identity management challenge faced by today's enterprise customers. Venafi delivers a solution that integrates with industry-leading Entrust nShield HSMs, on premises or as a service, to leverage strong hardware-based signing and encryption keys throughout the enterprise. Together Venafi and Entrust allow organizations to generate, store, and use keys securely – without private key material ever having to leave the HSM. These capabilities make it possible for enterprises to ensure the consistent use of the strongest cryptographic keys possible.

Why use Entrust nShield HSMs with Venafi?

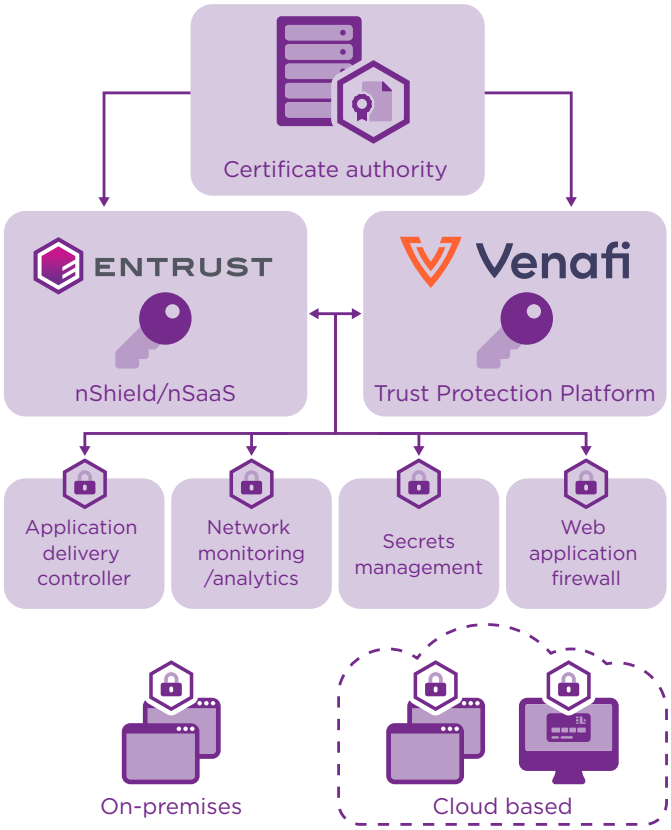
Cryptographic keys underpin the security of enterprise IT systems. Keys handled outside the protected boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromises. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield® Connect on-premises HSMs and nShield as a service (nSaaS) secure the generation and storage of the private keys used by the Venafi Platform. nShield HSMs enforce key use policies, separating security functions from administrative tasks. Doing so provides the highest level of security and assurance against key compromise and theft, while delivering scalability, flexibility, and efficiency.

Protecting the bigger ecosystem: machine identities are vulnerable and under attack

Today's authentication and encryption landscape includes a multitude of applications. Machine identities ensure trust across on-premises and cloud based deployments, from virtual private networks (VPNs), to application delivery controllers (ADCs), web application firewalls (WAFs), and performance monitoring and analytics software. A variety of attack vectors including downloadable code, weak or compromised keys, and expired certificates protect organizational secrets and control access to systems, applications, and data. Not only are these vectors a growing target of exploitation, but adoption of cloud, containers, and DevOps models can make it even harder to protect these ecosystems.

Venafi and Entrust deliver automated and secure cryptographic key orchestration

Venafi Trust Protection Platform and Entrust nShield HSMs, deployed together with leading machine identity providers like CAs, and machine identity consumers like ADCs, WAFs, network monitoring and analytics software, and secrets management applications, can significantly enhance the orchestration and security of machine identities.



The Venafi Trust Protection Platform together with Entrust nShield HSMs orchestrates secure machine identities across today's distributed computing deployments.

nSaaS: nShield as a Service, Entrust's subscription based HSM as a service available in the cloud.

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.

Venafi

Venafi brings to market machine identity management, securing machine-to-machine connections and communications. Venafi protects machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, code signing, mobile, and SSH. Venafi delivers innovative solutions for the world's most demanding, security-conscious Global 5000 organizations and government agencies. **venafi.com**

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

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223