Entrust nShield HSMs meet the requirements for NSA's Commercial Solutions for Classified (CSfC) Key Management Annex

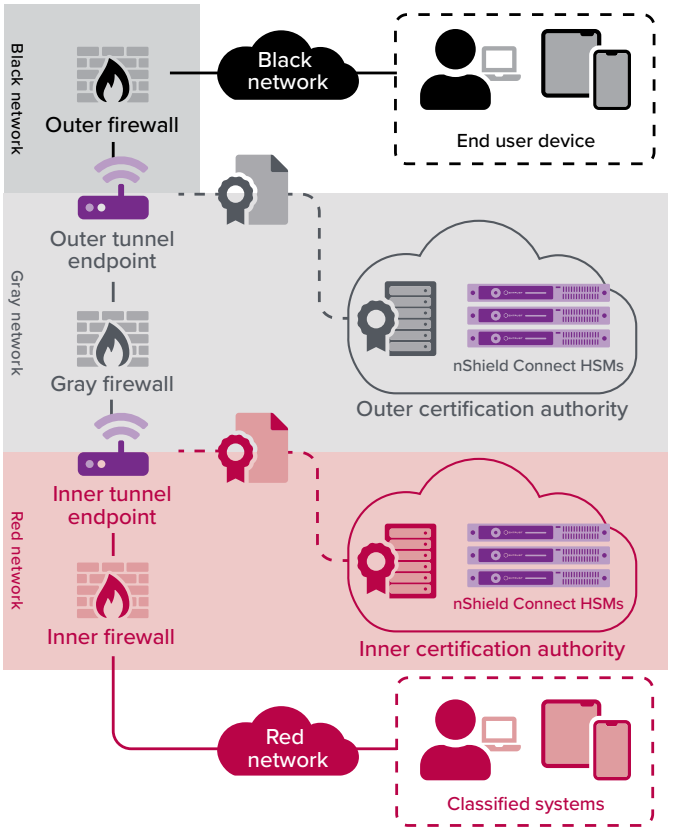
Deploy and maintain NSA-approved solutions with Entrust hardware security modules integrated with validated PKI applications

HIGHLIGHTS

- Support for CSfC approved certificate authority solutions provided by Red Hat and Information Security Corporation
- Can be clustered to scale cryptographic functions without sacrificing security
- Robust support for all Commercial National Security Algorithm Suite (CNSA) algorithms

The problem: high cost of protecting classified data

Traditionally, delivering solutions to the US Government to protect classified data has proven cumbersome and expensive. Few products were available and approved to protect this type information; lack of competition and high development costs made these solutions expensive and lacking in modern features. Acquisition and approval delays for security solutions can seriously weaken the US Government's security posture.



LEARN MORE AT ENTRUST.COM/HSM

Meet the requirements for the CSfC Key Management Annex

The challenge: reducing cost and modernizing capabilities to protect classified data

The National Security Agency's Commercial Solutions for Classified (CSfC) program aims to modernize its approach for protecting classified data by first looking to commercial-off-the-shelf (COTS) solutions. NSA believes **"properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications[1]".** The CSfC framework includes a list of approved COTS products and capability packages to help system integrators deliver solutions that protect classified data. Trusted Integrators for CSfC face the challenge of selecting approved COTS products that meet program requirements and then delivering a complete security solution.

The solution: Entrust HSMs meet the requirements of the NSA CSfC key management annex

The Key Management (KM) Requirements Annex is a core Capability Package for CSfC, and details how CSfC solutions may use CNSA-approved asymmetric algorithms and x.509 certificates to establish dual-layer (inner and outer) encryption tunnels for securing classified data in-transit at levels up to TOP SECRET. The nShield® family of HSMs increases the assurance level of PKI deployments and helps customers meet regulatory requirements and government mandates, including all HSM requirements defined by the KM Capability Package. Your investment in nShield HSMs is future-proofed against new requirements such as quantum resistant algorithms.

Why use Entrust nShield HSMs with CSfC solutions?

Combining a commercial-first approach with industry standard cryptographic algorithms greatly reduces delivery time of complex security solutions. It also reduces the government's dependency on expensive and often poorly maintained custom-built solutions.

For customers deploying PKIs, Entrust offers training, deployment services, health checks, documentation services, and key migration services to help your organization meet the challenges of successfully deploying an approved CSfC solution.

The nShield family of HSMs meets all HSM requirements defined by the NSA CSfC Key Management Capability Package, including:

- KM-12[2] which states "Private keys associated with on-line (i.e., CA is network-accessible), locally run Outer and Inner CAs must be protected using Hardware Security Modules (HSMs) validated to Federal Information Processing Standards (FIPS) 140-2 Level 2."
- nShield HSMs support all of the algorithms listed in the CNSA suite, as approved in CNSS Advisory Memorandum 02-15
- Entrust is actively planning support for quantum-resistant algorithms once final selections are approved for the CNSA suite
- All new algorithms are available via firmware updates, no new hardware required - your investment is safe!

1. Source: https://www.nsa.gov/resources/everyone/csfc/

2. Source: https://www.nsa.gov/resources/everyone/csfc/capability-packages

Meet the requirements for the CSfC Key Management Annex

nShield HSMs integrate with CSfC certified PKI solutions from Red Hat and Information Security Corporation to provide comprehensive logical and physical protection of critical key material protecting classified data.

Entrust nShield HSMs enable US Government customers and CSfC Trusted Integrators to deploy security solutions that:

- Use a hardened FIPS 140-2 level 3 validated cryptographic module to protect highly sensitive cryptographic key material
- Perform secure cryptographic processing using FIPS validated Random Number Generation (RNG)
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)
- Enforce robust access control and key use policies, so they are only used for their authorized purpose
- Ensure high-availability of keys by using sophisticated management, storage, and redundancy feature

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.

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**

About Red Hat

Red Hat is a leading provider of open source solutions for the enterprise. Solutions include Red Hat Enterprise Linux, Red Hat OpenStack Platform, and Red Hat Certificate System as well as a broad range of management and services. Entrust nShield HSMs are certified with the Red Hat Certificate System.

For more information visit **www.redhat.com**

About Information Security Corporation

Information Security Corporation (ISC) specializes in the design and development of cybersecurity solutions for PKI credential management, automated provisioning of relying applications, encryption, and authentication. ISC is heavily focused on the development of a host of certificate lifecycle management applications and cryptographic web services that comprise the CertAgent product.

For more information visit **infoseccorp.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