Trusted Cyber Technologies

THALES
Building a future we can all trust

Thales TCT Luna HSMs for Commercial Solutions for Classified (CSfC)

What is CSfC?

Commercial Solutions for Classified (CSfC) is a program that enables commercial products to be used in layered solutions to protect classified information. This speeds up the deployment timeline so that a solution can be fielded in months, versus years. The program was designed to allow simultaneous use of multiple unclassified commercial off the shelf (COTS) products instead of classified, Type 1 U.S. Government accredited products to secure classified data within government deployments.

CSfC promotes the protection of critical data with layered encryption technologies. A layered encryption approach is most effective when each layer can stand independently relative to their design, implementation, and operational deployment. There are currently five approved CSfC Capability Packages, each of which defines solution level specifications that include all operational requirements; configuration requirements and architecture, requirements for site testing, and rules for using/maintaining/protecting/disposing of solutions.

The Role of Hardware Security Modules (HSMs) in CSfC

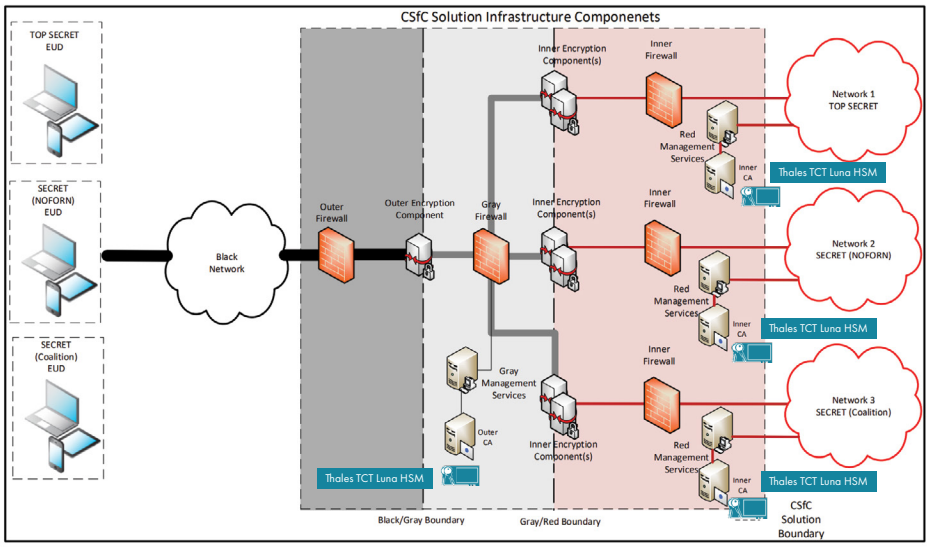
Recognizing the critical role key management plays in securing all cybersecurity solutions, a change was made to the Capability Packages moving all key management requirements to a dedicated Key Management Requirements Annex. Consolidation of requirements common across multiple Capabilities Packages provides an additional level of efficiency for both trusted integrators and evaluators that work across multiple solutions.

Following the CSfC security principles of using multiple independent security layers, the Key Management Requirements describe the need to implement at least two separate Certificate Authorities (CA) running on separate machines and networks for issuing the PKI certificates within the solution. The Outer CA and Inner CA are used to issue certificates to the Outer and Inner Encryption Components, respectively. For CSfC solutions that support multiple classified enclaves, each enclave will have a separate Inner CA to ensure cryptographic isolation of the enclaves.

With a long history of securing the private key of Certified Authorities, HSMs are a perfect fit into every CSfC solution that uses CAs. It is noted that use of an HSM to secure the CA private keys is not only a best-practice, but it is specifically required by CSfC. Due to the separation requirements, each CA would use a dedicated HSM to hold its private key. This is illustrated in the following diagram from the CSfC Key Management Requirements Annex, modified to show the location of an HSM with each CA.

KM-12 (Key Management Requirements Annex): Private keys associated with on-line (i.e., CA is network-accessible), Outer and Inner CAs must be protected using Hardware Security Modules (HSMs) validated to Federal Information Processing Standards (FIPS) 140-2 Level 2.

Ref. National Security Agency CSfC Key Management Requirements Annex v2.0, Figure 4



Proven Integrations

Thales TCT Luna HSMs integrate with industry-leading technology vendors to provide seamless solutions meeting the stringent security requirements established by the U.S. Government. With our U.S. based development and support staff, as well as a complete U.S. supply chain, our HSMs provide the hardened security needed to meet federal standards. We provide fully vetted, step-by-step integration guides for our broad partner ecosystem of out-of-the-box integrations As part of the Thales TCT Technology Partner Program, Thales TCT provides extensive and on-going technical integration support for the two products currently listed on the CSfC approved Certificate Authority Components List: ISC CertAgent and Red Hat Certificate System.

About Information Security Corporation (ISC)

ISC is headquartered in Oak Park, IL with additional sales offices in Rochester, NY and Arlington, VA. Development offices are located in Oak Park, IL and Santa Cruz, CA. The company was founded in 1989 to develop and market data security products based on public key cryptography. ISC has provided cutting-edge PKI-based security solutions to the world's most security conscious organizations for more than thirty years. ISC's CertAgent is a NIAP-validated and CSfC-approved X.509 certificate authority that integrates with Thales TCT's FIPS 140-2 Level 3 Luna T-Series HSM to provide government organizations with a highly secure and robust PKI solution to meet all needs. Learn more at infoseccorp.com.

About Red Hat

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT. Red Hat's Certificate System is a NIAP-validated and CSfC-approved X.509 certificate authority that integrates with Thales TCT's FIPS 140-2 Level 3 Luna T-Series HSM to provide government organizations with a highly secure and robust PKI solution to meet all needs. Learn more at redhat.com.

Thales TCT Luna HSMs Address CSfC Requirements

Thales TCT's Luna HSMs are the choice for government agencies when generating, storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high assurance, tamper-resistant Luna T-Series HSM is designed, developed, manufactured, sold, and supported in the United States exclusively by Thales TCT. Our HSMs address the CSfC Capability Package Key Management requirements

Key Benefits

- **Secure**- FIPS 140-2 Level 3 certification
- **Protected** - Keys-in-hardware approach protects the entire life-cycle of keys within the FIPS 140-2 Level 3 validated confines of the HSM
- **Approved** - CNSS approved for use in National Security Systems
- **Compliant** - Full support for NSA Commercial National Security Algorithm (CNSA) Suite
- **Effective** - Support for FIPS-approved and NIST recommended algorithms, modes, curves, and key sizes for RSA, DSA, Diffie-Hellman, AES, SHA-2 family, and Elliptic Curve Cryptography (ECC)
- **Extensible** - Crypto agile architecture supports in-field introduction of new crypto algorithms
- **Quantum Ready** - NIST 800-90A compliant Hardware Random Number Generator with Classic hardware RNG entropy or Quantum RNG entropy
- **Powerful** - Industry-leading cryptographic performance

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit thalestct.com.

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com