

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

thalestct.com

THALES
Building a future we can all trust

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 four approved CSfC Capability Packages, each of which outlines overall customer solution architecture requirements as well as specific device configurations.

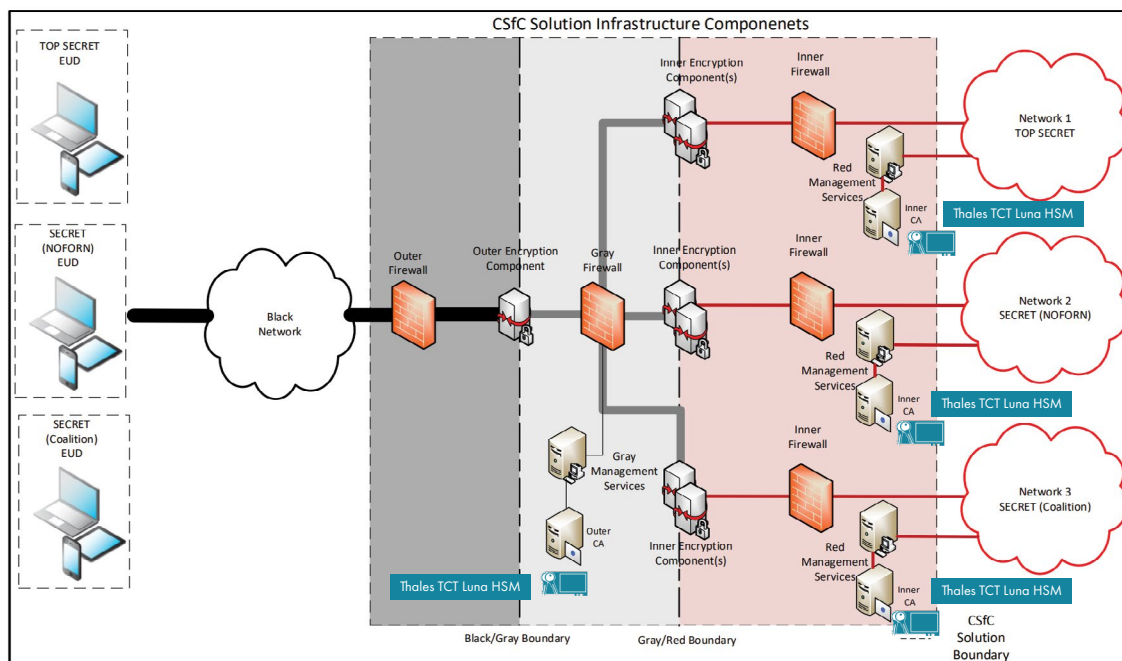
The Role of Hardware Security Modules (HSMs) in CSfC

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 must 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. Use of an HSM to secure the CA private keys is not only identified as a best-practice, it is specifically required per the CSfC Key Management Requirements Annex. Due to the separation requirements, each CA used 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.



Ref. National Security Agency CSfC Key Management Requirements Annex v2.1, Figure 5

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 HSMs validated to Federal Information Processing Standards (FIPS) 140-2/3 Level 2 or greater.

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.

Luna T-Series HSM Key Benefits

- **Secure** - FIPS 140 Level 3 certification
- **Approved** - CNSS approved for use in National Security Systems
- **Protected** - Keys-in-hardware approach protects the entire life-cycle of keys within the FIPS 140 Level 3 validated confines of the HSM
- **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, Diffie-Hellman, AES, SHA-2/3 families, and Elliptic Curve Cryptography (ECC)
- **Crypto Agile** - Supports in-field introduction of new crypto algorithms such as the NIST selected PQC algorithms
- **Quantum Enhanced Keys** - NIST 800-90A compliant Hardware Random Number Generator with Classic hardware RNG entropy or Quantum RNG entropy
- **Powerful** - Industry-leading cryptographic performance

Proven Integrations

Thales TCT Luna HSMs integrate with industry-leading technology vendors to provide seamless solutions that meet 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 products listed on the CSfC approved Certificate Authority Components List:

- ISC CertAgent
- Red Hat Certificate System
- Keyfactor EJBCA Enterprise

Each of these partners offer a NIAP-validated and CSfC-approved X.509 certificate authority that integrates with Thales TCT's FIPS 140 Level 3 Luna T-Series HSM to provide government organizations with a highly secure and robust PKI solution to meet all needs.

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 www.thalestct.com