Solution Brief

Hardware-Backed Zero Trust for Classified Data: Virtru Data Security Platform + Thales TCT Luna T-Series HSMs

thalestct.com

The Challenge

Protecting classified data demands more than encryption—it demands certainty about where your keys live. Even with robust attribute-based access control and policy enforcement, encrypted data is only as secure as the cryptographic keys protecting it. Software-based key storage leaves those keys vulnerable. For agencies handling classified information, hardware-backed key protection isn't optional—it's mandated by FedRAMP, FISMA, and NIST standards. The challenge extends further: agencies must also enable cross-domain collaboration while meeting intelligence community requirements for metadata handling and classification markings.

The Solution

Virtru Data Security Platform with Thales Trusted Cyber Technologies (TCT) Luna T-Series HSMs delivers end-to-end data protection with hardware-backed key security. The integration ensures cryptographic keys are generated and protected within FIPS 140 Level 3 validated hardware—eliminating software key exposure while enabling secure collaboration across classification boundaries and coalition partners.

Deployment Modes

The integration supports two modes, enabling organizations to balance operational requirements with security assurance:

Envelope Mode: A root symmetric key stored in the HSM wraps the Key Access Service private keys before they are stored in the platform database. AES-based symmetric key wrapping provides hardware-backed protection while maintaining operational flexibility.

Delegated Mode: Key Access Service private keys never leave the HSM. All cryptographic operations—including RSA key generation (2048/3072/4096 bit), data encryption key wrapping, and unwrapping—occur directly within the hardware security module. No key material is exposed outside the secure boundary.

Standards Compliance

The platform supports ACP 240 Zero Trust Data Format (ZTDF), Intelligence Community metadata requirements (IC-EDH), and NATO interoperability standards (STANAG 5636). Agencies can enforce attribute-based access control policies using classification markings, releasability controls, and dissemination restrictions, with cryptographic key material maintained in hardware that meets the highest security certifications.

Key Benefits

Hardware-Based Secure Key Storage: Master encryption keys are generated within FIPS 140 Level 3-validated hardware and protected using hardware-backed key wrapping (envelope mode) or complete HSM retention (delegated mode), eliminating software-based key exposure risks.

Flexible Key Protection Modes: Support for both envelope mode (HSM-wrapped keys in database) and delegated mode (keys never leave HSM) enables organizations to balance operational requirements with maximum security assurance.

FIPS-Validated Cryptographic Operations: Cryptographic operations leverage FIPS 140 Level 3-validated HSM capabilities, supporting RSA cryptography (delegated mode) and AES symmetric-key operations (envelope mode) within the secure hardware boundary. Luna T-Series HSM is approved by CNSS for use in National Security Systems PKI.

ACP 240 ZTDF Compliance with Hardware Key Security: Native support for the Zero Trust Data Format, combined with hardware-backed key management, enables Intelligence Community metadata handling (IC-EDH) and NATO STANAG 5636 interoperability, including classification markings, releasability controls, and dissemination restrictions.

Cross-Domain Collaboration: Attribute-based access control with hardware-backed keys enables secure data sharing across classification levels, agencies, and coalition partners while maintaining policy enforcement.

Regulatory Compliance: Meet FedRAMP, FISMA, NIST 800-53, and Intelligence Community Directive requirements with a platform designed for federal security mandates.

Trusted U.S. Source: Both Virtru and Thales TCT develop, manufacture, and support solutions entirely within U.S. boundaries, providing a completely trusted domestic supply chain.

High Availability Architecture: Multiple Luna T-Series HSMs can be deployed in high-availability configurations to ensure continuous cryptographic service availability for mission-critical operations.

Flexible Deployment Models: Support for cloud, on-premises, and hybrid environments with HSM integration across AWS GovCloud, Azure Government, and air-gapped networks.

About Virtru

Virtru is pioneering the shift from network-centric to data-centric security — embedding protection directly into data so mission owners maintain control wherever sensitive information is shared. The Virtru Data Security Platform is built on OpenTDF, an open standard evolved from technology developed at the NSA by co-founder Will Ackerly, and supports ACP 240, the Five Eyes-ratified Zero Trust standard for secure coalition operations. Trusted by over 6,000 public and private sector organizations — including the U.S. Department of Defense, JPMorgan Chase, and Salesforce — Virtru enables secure collaboration across classification boundaries at mission speed, with integrations across leading defense, cloud, and cross-domain solution providers. Virtru is headquartered in Washington, D.C.

Virtru Data Security Platform

Virtru Data Security Platform is an enterprise-grade, data-centric security solution. Building on OpenTDF's foundational core services and TDF data encoding specification, Virtru developed additional capabilities to deliver a mission-ready platform for national security and intelligence community requirements:

- **Standards support** for IC-TDF, ACP 240 Zero Trust Data Format (ZTDF), Intelligence Community metadata (IC-EDH, ISM, IC-ID), and NATO STANAG 5636—including classification markings, releasability controls, and dissemination restrictions that travel with protected data
- **Ready-to-deploy policy enforcement** across collaboration applications, data analytics pipelines, and agentic AI workflows
- **Automated tagging** with native support to read and output STANAG and Intelligence Community handling metadata, along with support for reading metadata generated by third-party tagging systems like Fortra and JanusNet
- **Universal identity integration** with any OIDC/OAuth2 provider

With native HSM integration via PKCS#11 and support for Thales TCT Luna T-Series, organizations maintain full key sovereignty—ensuring cryptographic keys remain under customer control within FIPS 140 validated hardware. Flexible deployment across cloud, on-premises, and air-gapped environments enables the Virtru Data Security Platform to meet the most demanding operational requirements.

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 cybersecurity solutions for the U.S. Federal Government. Thales 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.

Thales TCT Luna T-Series HSM

The Luna T-Series HSM provides FIPS 140 Level 3 validated cryptographic key protection with tamper-resistant hardware, supporting a wide range of cryptographic algorithms and key types. As a dedicated U.S. source, Thales TCT develops, sells, manufactures, and supports core data security solutions solely within the boundaries of the United States, providing federal agencies with a completely trusted domestic source for hardware security modules.

For More Information

Contact Us For more information about Virtru Data Security Platform with Thales TCT Luna Network HSM integration, visit:

- Virtru: www.virtru.com
- Thales TCT: www.thalestct.com