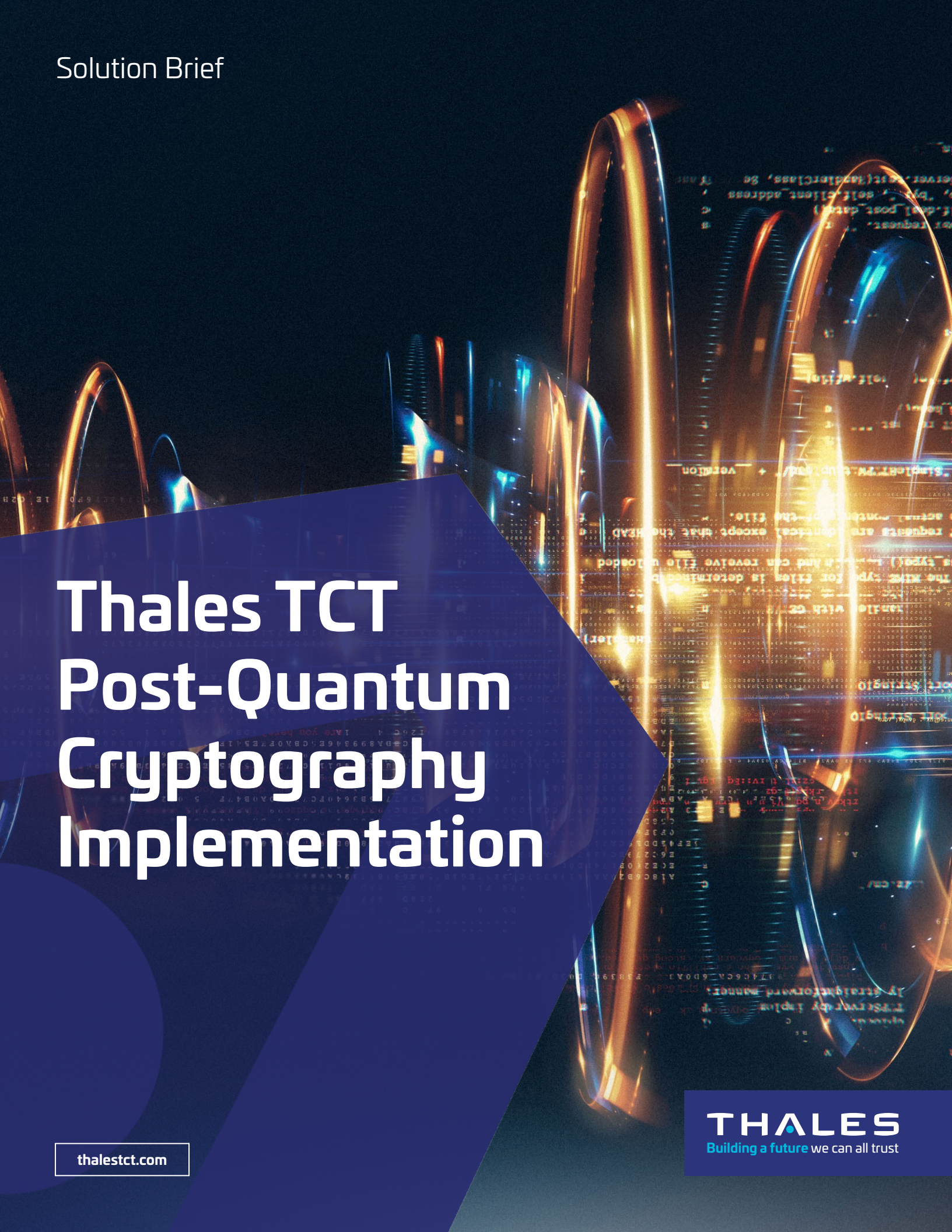
Solution Brief



Thales TCT Post-Quantum Cryptography Implementation

thalestct.com

THALES
Building a future we can all trust

THALES

Executive Summary

Thales Trusted Cyber Technologies (TCT) is addressing the quantum computing threat by integrating Post-Quantum Cryptography (PQC) into its high-assurance cryptographic solutions, including Luna T-Series Hardware Security Modules (HSMs), CN Series Network Encryptors, CipherTrust Data Security Platform, and authentication smart cards. By aligning with NIST-standardized PQC algorithms, leveraging crypto-agility, and collaborating with the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), through a Cooperative Research and Development Agreement (CRADA), Thales TCT ensures quantum-resistant security for U.S. Government intelligence, defense, and civilian agencies. This brief outlines Thales TCT's strategy, implementation approach, and roadmap to deliver future-proof, compliant cryptographic solutions.

Background

Quantum computing advancements pose a significant risk to traditional cryptographic algorithms like RSA and ECC, which could be broken by quantum algorithms such as Shor's. NIST has responded by standardizing PQC algorithms, including ML-KEM, ML-DSA, SLH-DSA, LMS, and HSS, to secure data against quantum threats. Thales TCT, a leader in cryptographic solutions for U.S. Federal agencies, is proactively adopting PQC to protect sensitive data and ensure compliance with emerging standards such as the U.S. National Security Memorandum on PQC.

Solution Overview

Thales TCT's solutions leverage the company's work with NIST and NSA to align with federal standards and incorporate crypto-agile frameworks to adapt to evolving PQC requirements. Thales TCT's PQC implementation focuses on embedding NIST-standardized quantum-resistant algorithms into its product portfolio to ensure crypto-agility and high-assurance security. Key products include:

- **Luna T-Series HSMs:** Thales TCT's HSMs support quantum-resistant algorithms like LMS and HSS for code signing, ML-KEM for protocols using key encapsulation, and ML-DSA for PKI, web server authentication, smartcard management, and other use cases.
- **CN Series Network Encryptors:** Although data-in-motion security is natively quantum resistant, Thales TCT's Network Encryptors will be upgraded to utilize PQC algorithms for secure management and key exchange protocols.
- **CipherTrust Data Security Platform:** To facilitate a smooth transition to PQC, Thales TCT's wide range of connectors and key management solutions are being enhanced to support PQC algorithms.
- **Smart Cards:** A fundamental element of most Identity and Access Management systems, Thales TCT is developing smart cards capable of performing ML-DSA signatures in support of document signing, email security, web authentication, and workstation smartcard logon.

Implementation Approach

Thales TCT is adopting a multi-pronged strategy to integrate PQC across its solutions:

1. **Adoption of NIST PQC Algorithms:** Starting with integration of pre-standardized algorithms like CRYSTALS-Kyber and Dilithium into HSMs and network encryptors, Thales TCT has been at the forefront of making PQC capable products available to customers. With NIST PQC standards now in place, Thales TCT is continuing its PQC leadership by implementing the standardized algorithms and protocols across the entire product portfolio.
2. **Crypto-Agility:** Thales TCT designs systems to seamlessly transition from legacy to quantum-resistant algorithms, minimizing disruption and ensuring compliance with future mandates.
3. **NIST Collaboration:** As a founding participant in the NIST National Cybersecurity Center of Excellence (NCCoE) Migration to PQC project, Thales TCT has been collaborating with NIST and industry partners since 2022 to test pre-standards PQC implementations for interoperability and performance. Thales TCT used these results to accelerate PQC product development while ensuring the developing ecosystem of PQC implementations is standards compliant and interoperable.
4. **Meeting Government Timelines:** The NSA issued Commercial National Security Algorithms (CNSA) 2.0 guidelines requiring National Security Systems (NSS) perform a phased migration to PQC between 2024 and 2033. Thales TCT is committed and on track to offer customers crypto-agile products with PQC capabilities to allow them to meet that timeline.
5. **Customer Enablement:** Thales TCT provides tools, documentation, and training to help customers assess cryptographic inventories and transition to PQC, aligning with Zero Trust frameworks and compliance with PQC migration policies.

Benefits

- **Quantum-Resistant Security:** Protects sensitive data against current and future quantum threats.
- **Compliance Readiness:** Aligns with NIST standards and federal mandates, simplifying adoption for US federal agencies.
- **Seamless Transition:** Enables smooth algorithm updates without hardware or software overhauls with crypto-agile solutions.
- **High Assurance:** Ensures compliance with stringent government and industry requirements with hardware-based security.
- **Proactive Protection:** Positions customers ahead of quantum computing advancements with early adoption of PQC.

Roadmap

Thales TCT's PQC implementation follows a phased approach:

- **2025-2026:** Expand support for NIST PQC algorithms across the entire Thales TCT product portfolio via firmware and software updates.
- **Ongoing:** Continue NIST collaboration to validate and refine PQC implementations, incorporating emerging standards.
- **Customer Support:** Deliver migration tools, workshops, and guidance to facilitate PQC adoption in line with anticipated federal deadlines.

Organizations are encouraged to contact Thales TCT for tailored PQC transition plans. Visit thalestct.com or contact info@thalestct.com for details.

Conclusion

Thales TCT is leading the transition to quantum-safe cryptography by integrating PQC into its trusted solutions. Through NIST-aligned algorithms, crypto-agility, and strategic partnerships, Thales TCT empowers customers to secure critical systems against quantum threats while maintaining compliance and operational efficiency. By adopting Thales TCT's PQC-ready solutions, organizations can confidently navigate the quantum era.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

Contact us - For office location and contact information, please visit thalestct.com/contact-us