Compliance Brief

THALES

CYBERSECURITY

Strengthening the Fundamental Security Pillars for Caliptra

cpl.thalesgroup.com

THALES

CYBERSECURITY

Caliptra is an open-source Root of Trust (RoT) architecture designed for datacenter System-on-Chip (SoC) platforms. It provides a unified, open-source building block that can be integrated directly into any modern datacenter-class chip (CPUs, GPUs, TPUs, DPUs, or smart SSDs).

What is Inside Caliptra?

Caliptra is actual and usable code, which provides:

1. **Hardware RTL (Silicon Logic):** The actual blueprints for the physical circuit block, built around an open-source **RISC-V** processor core.
2. **Cryptographic Accelerators:** Dedicated hardware to process security algorithms quickly without bogging down the main CPU. Recent updates (Caliptra 2.1) even feature **Post-Quantum Cryptography** (like ML-DSA and ML-KEM) to protect against future quantum computer attacks.
3. **Firmware:** The immutable ROM and runtime firmware needed to operate the security block.

By making this architecture transparent and open-source, Caliptra serves as the "security anchor" for a server or accelerator chip, providing a trusted foundation on which higher-level security services can be built.

What is Caliptra?

Caliptra is an open-source hardware security project that provides a standardized **Silicon Root of Trust (RoT)**. Founded in 2022 by a powerhouse coalition including AMD, Google, Microsoft, and NVIDIA, it is managed by the CHIPS Alliance and the Open Compute Project (OCP).

How Thales Aligns with Caliptra's Specification

Thales' HSM Solutions can help organizations align with Caliptra's specification for cryptographic infrastructure.

Requirements	How Thales helps
Caliptra: A Datacenter System on a Chip (SoC) Root of Trust (RoT)	
Compliance and certification requirements • It is relevant when a cloud provider wants to **FIPS-certify (FIPS 140-3 L3)** PCIe link encryption in transit rooted to an ASIC identity emanating from a Caliptra instance.	• **Cryptographic module certification** Offer FIPS 140-3 Level 3 validated HSMs which serve as the trust anchor for manufacturing PKI, certificate issuance, signing operations, and lifecycle key management supporting a FIPS-compliant ecosystem.
Known Answer Test (KAT) support • To certify a cryptographic module, pre-operational self-tests must be performed when the system is booted. **Implementing KATs** is required for **FIPS certification**.	• **Mandatory cryptographic self-tests for certification** Provide independently validated cryptographic services and self-test mechanisms that align with FIPS operational requirements for the supporting PKI infrastructure.
NIST Compliance Requirements	
• The UDS seed and field entropy MUST be statistically uniquely generated using a cryptographically secure random number generator **(CSRNG)** seeded by an entropy source compliant with **NIST Entropy Source Certification SP 800-90B**. • Caliptra Checklist and Evaluation Methodology	• **Secure generation of device identities and secrets** Provide validated entropy generation capabilities for generating and protecting manufacturing keys, CA keys, and provisioning secrets. • **Unique device identity root secret** Generate, wrap, inject, or protect device identity material and associated certificate issuance workflows during manufacturing/provisioning.

Requirements	How Thales helps
• The **IDEVID certificates**, including CA certificates, MUST adhere to specified formats and cryptographic standards (e.g. key sizes and algorithms as per NIST guidelines). • Caliptra Checklist and Evaluation Methodology	• **Device identity and attestation** Generate and protect the Root CA and Intermediate CA keys used to issue IDevID certificates that meet NIST cryptographic requirements. • **Trust establishment** Secure CA private keys and support certificate lifecycle operations for Caliptra device identity ecosystems.
Post-Quantum Cryptography (PQC)	

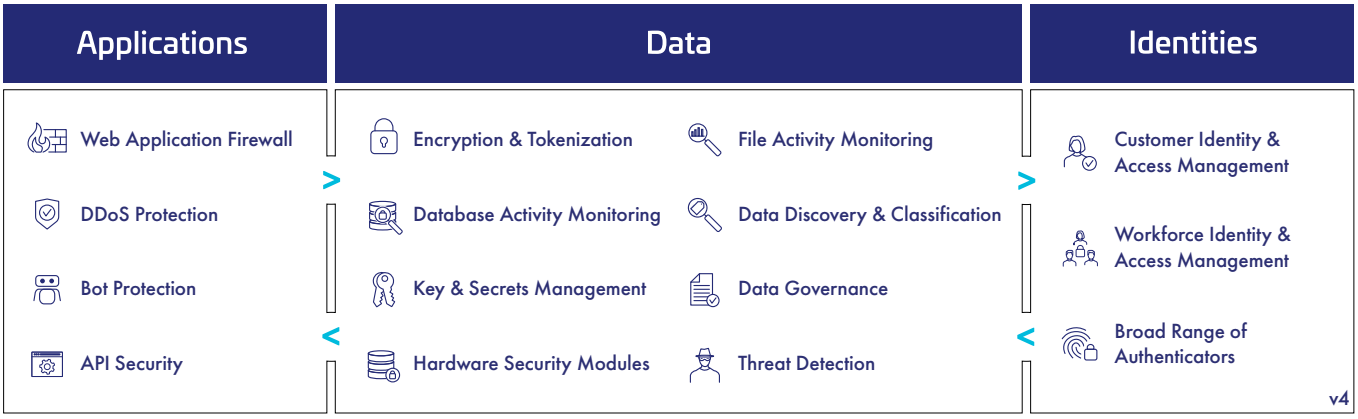
• Caliptra 2.x targets **PQC compliance**
  ◦ Caliptra Trademark Audit Process
• Caliptra includes **ML-DSA (FIPS 204)** PQC implementation through Adams Bridge.
  ◦ Adams Bridge Hardware Specification - Post-Quantum Cryptography IP Core (ML-DSA (FIPS 204)
  ◦ Adams Bridge README
	• **Future quantum-resistant security**
	Support NIST-approved ML-KEM (FIPS 203) and ML-DSA (FIPS 204). This aligns with Caliptra's planned PQC evolution and enables future PQC-enabled provisioning and certificate workflows.
	• **PQC signing and attestation**
	Act as the secure backend platform for PQC certificate authorities and signing infrastructure while Caliptra integrates PQC capabilities on-device.

Caliptra 1.x: LMS & ECDSA required • Caliptra has an option to require **LMS signatures** in addition to **ECDSA signatures**. • It is recommended that the LMS trees are created from **multiple HSMs** that are geographically distributed.	• **Hardware protection for signing keys:** Provide a FIPS 140-3 Level 3 validated environment for protecting private signing keys used in firmware signing and attestation workflows. • **Distributed trust infrastructure:** Support deployment in geographically distributed environments, enabling resilient and highly available cryptographic services that align with Caliptra's recommendation for distributed LMS tree creation. • NIST CAVP (PQC) Validation (#39968)
Caliptra 2.0: MLDSA, ML-KEM, ECDSA, ECDH required • Caliptra has an option starting in **2.0** to use **ML-DSA-87** signatures in addition to **ECDSA** to support FIPS 204 and CNSA 2.0 requirements for category 5. • Caliptra provides cryptographic services to support **ML-KEM (in addition to ECDH)** key exchanges.	• **Post-quantum digital signatures:** Support ML-DSA (FIPS 204), providing hardware-backed protection for post-quantum signing keys used in certificate issuance, firmware signing, and attestation. • **Post-quantum key establishment:** Support ML-KEM (FIPS 203), enabling hardware-protected quantum-resistant key establishment for secure provisioning and cryptographic infrastructure. • NIST CAVP (PQC) Validation (#39968)
Common Cryptographic Module Requirements	
Strict requirements for **key generation and protection** • Caliptra Checklist - Asset Management - UDS seed protection requirements • Caliptra Hardware Specification - Key Vault	• **Secure storage and use of cryptographic keys** Provide hardware-backed protection for manufacturing, provisioning, attestation, and PKI keys. Caliptra Key Vault protects device-resident keys after provisioning.
Physical **tamper-resistance** and detection mechanisms • Caliptra Hardware Specification - Physical security features	• **Protection against physical attacks** Provide FIPS 140-3 Level 3 physical protection. Caliptra provides SoC-level physical security features within the device. Together, they create end-to-end protection from the backend trust anchor to the endpoint device.
Integrity **assurance for cryptographic operations** • Caliptra ROM Threat Model • Caliptra Security Assessment Report	• **Protection against firmware or cryptographic tampering** Protect signing keys used for firmware signing and attestation infrastructure. Caliptra verifies firmware integrity within the device root of trust.

Requirements	How Thales helps
Entropy **source certification** • Caliptra Checklist - Entropy Requirements - NIST SP 800-90B (entropy source validation) and NIST SP 800-90A (DRBG mechanisms) compliance • Caliptra: A Datacenter System on a Chip (SoC) Root of Trust (RoT)	• **Regulatory compliance** Support compliance requirements in the backend trust infrastructure with entropy generation and validated cryptographic modules.

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

Security for What Matters Most



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs and a secure Content Delivery Network (CDN).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us