

nQrux® Root of Trust

Product code: XIP7450B

nQrux® Root of Trust establishes device identity, protects cryptographic keys, and anchors secure boot and other security services for hardware systems. As the foundation of system security, it provides a trusted and immutable environment for critical security operations, ensuring that attackers cannot alter its contents or behavior. Secure Boot, firmware updates, device identity, and secure communication all rely on it. nQrux Root of Trust offers a streamlined and hardened architecture to protect against malicious compromise attempts.

KEY FEATURES

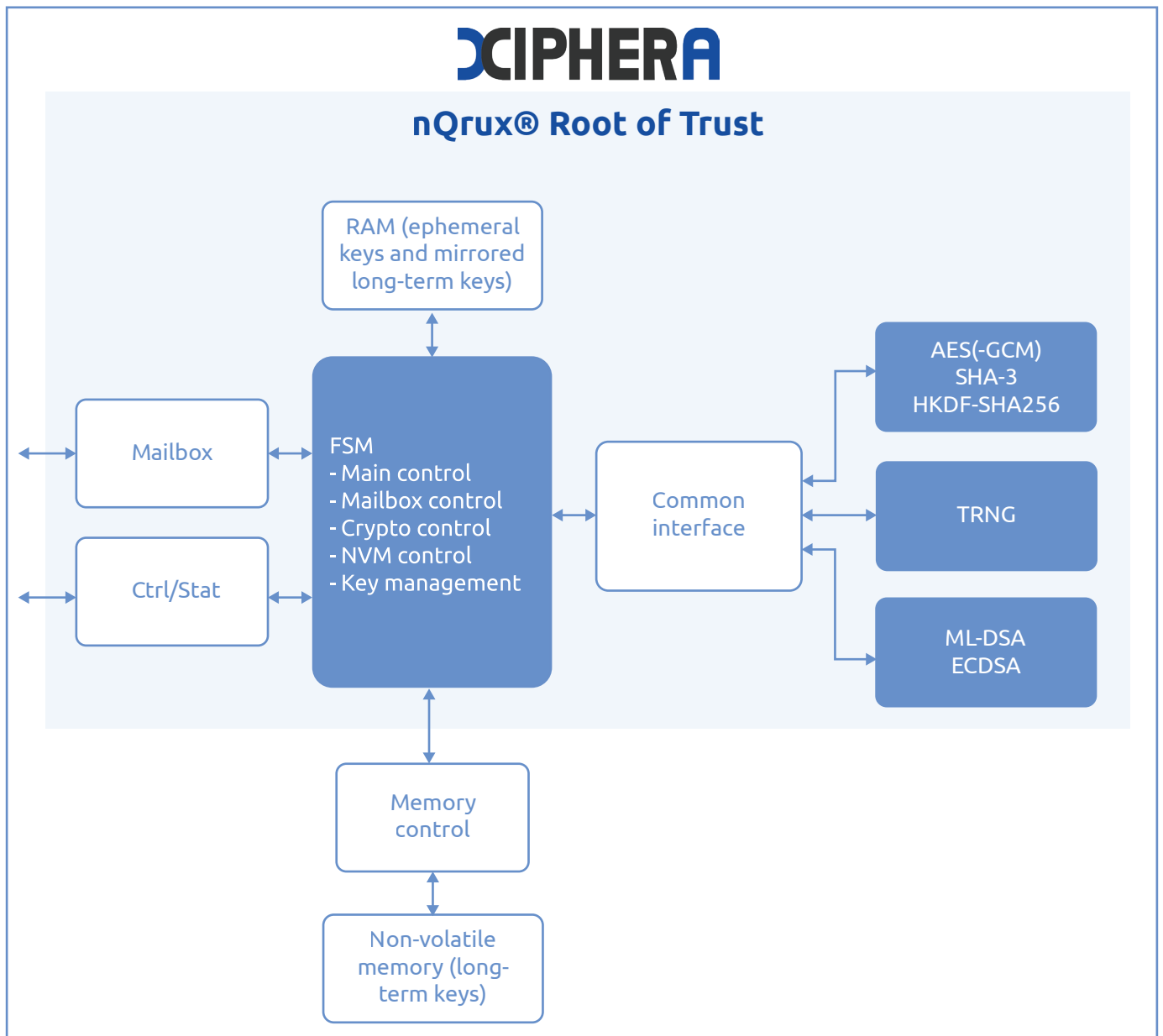
- ◉ **Trust anchor.** Upper architecture layers inherit their security from nQrux Root of Trust and rely on it as the foundation of system trust.
- ◉ **No processor.** Pure digital logic, no CPU, no software, a smaller attack surface.
- ◉ **Small and low power.** Hundreds of thousands rather than millions of gates in ASIC implementations, reducing silicon area and power consumption.
- ◉ **Smaller memory consumption.** No software or firmware means less memory is needed, reducing system resources and complexity.
- ◉ **Keys stay isolated.** Ephemeral keys in RAM, long-term keys in NVM, each user accessing only their own.
- ◉ **Protected interfaces.** AES256-GCM encryption against eavesdropping, manipulation, and replays.
- ◉ **Modern cryptography.** AES-GCM, elliptic curve cryptography, SHA-3, as well as quantum-resilient PQC algorithms.
- ◉ **Easy to integrate.** A 32-bit mailbox interface, configurable memory.
- ◉ **Vendor agnostic.** Implementable across FPGA, ASIC, and SoC-based system.

CRYPTOGRAPHIC OPERATIONS

- ◉ Key generation / derivation
- ◉ Diffie-Hellman key exchange
- ◉ ML-KEM key encapsulation/decapsulation
- ◉ Symmetric encryption
- ◉ Hashing
- ◉ Message authentication
- ◉ Signature generation/verification

USER AND DATA MANAGEMENT

- ◉ Users: Admin vs. Regular
- ◉ User-specific memory space (RAM + NVM)
- ◉ Slot-based storage with permission and usage policies for data and keys
- ◉ Commands via encrypted and authenticated Mailbox interface



APPLICATIONS

Quantum-resistant Root of Trust for:

- IoT and industrial automation
- Space and satellite systems
- Defence and mission-critical applications
- AI Infrastructures
- Data centres and edge



About Xiphera

Xiphera, Ltd, is a Finnish company designing hardware-based security solutions using standardised cryptographic algorithms. Our product portfolio consists of secure and efficient cryptographic Intellectual Property (IP) cores, designed directly for ASICs and FPGAs. Our strong cryptographic expertise, extensive experience in system design, and deep knowledge in the field of reprogrammable logic enable us to offer our customers peace of mind in a dangerous world.