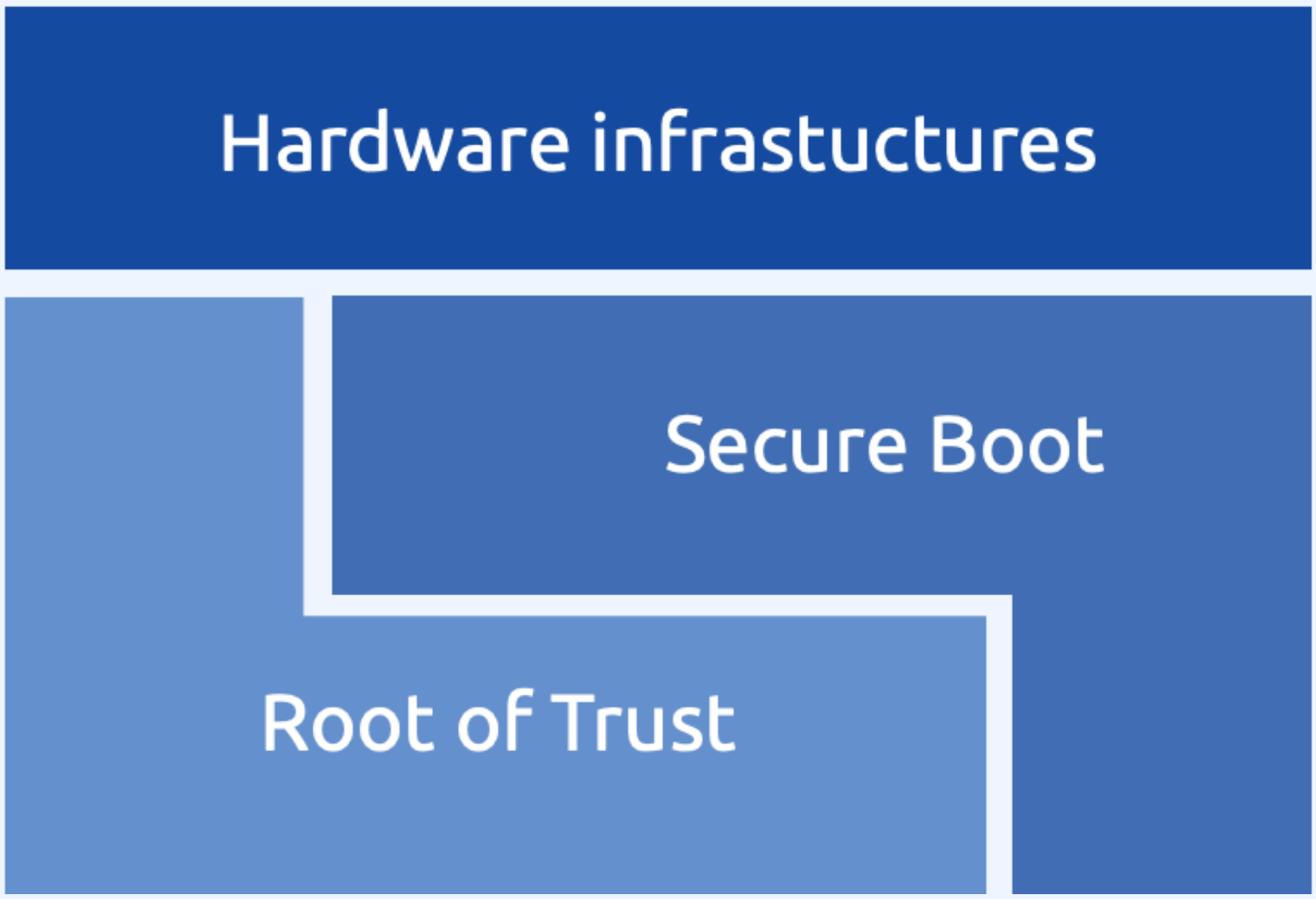
XIPHERA

# nQrux® Root of Trust

# Building trust into hardware

# Foundations for Digital Resilience

- Modern hardware platforms for IoT, cloud and AI environments need a secure foundation.
- Before a device can trust the firmware it runs, it needs a reliable way to verify its authenticity and integrity.
- A Root of Trust provides the foundation for security mechanisms such as Secure Boot, helping prevent unauthorized firmware from being accepted during startup.



# What does a Root of Trust  do?

A Root of Trust provides a trusted foundation for critical security functions, including device identity, cryptographic key protection, secure communication and Secure Boot.
By protecting the mechanisms these functions depend on, it helps establish trust in the device and the software it runs.

## What it does:



Establishes and supports device identity



Protects cryptographic keys and controls their use



Performs cryptographic operations

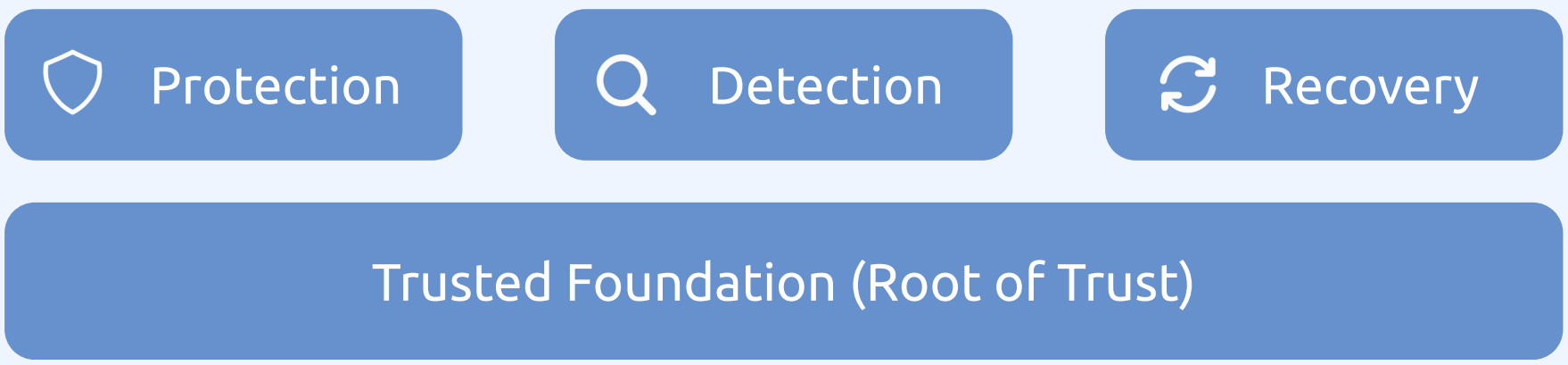


Provides a trust anchor for Secure Boot

# Why NIST considers Root of Trust important

- Security mechanisms depend on the trustworthiness of the components beneath them.
- NIST’s Root of Trust guidance emphasizes that these critical components must be secure by design.
- Hardware implementations need to be hardened against cyber threats

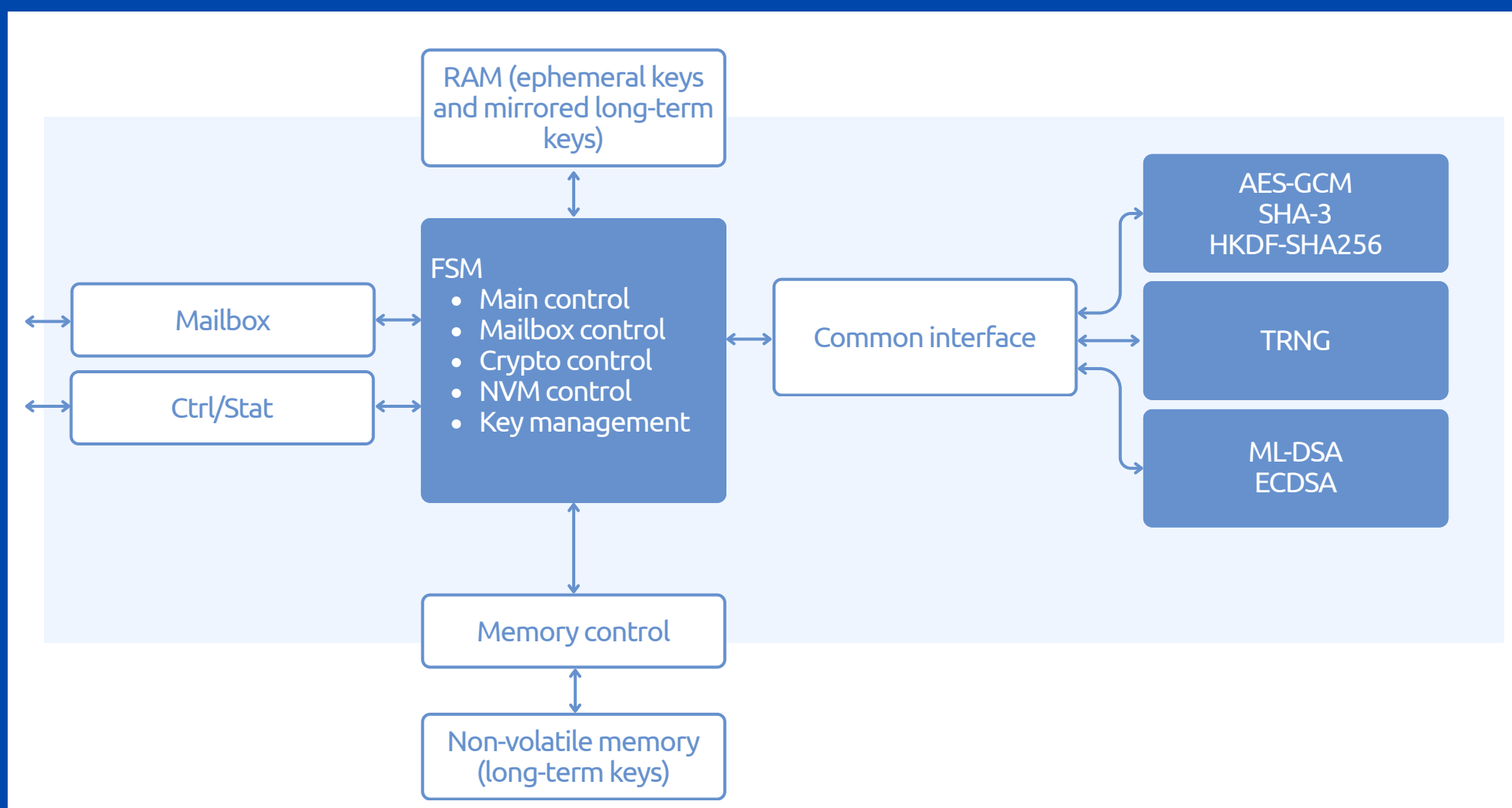
**Three Principles of Platform Firmware Resilience**




Conceptual illustration based on NIST SP 800-193.

*Source: NIST SP 800-193, Platform Firmware Resiliency Guidelines (2018), Sections 3.1 and 3.3.*

# Finite State Machine Based Root of Trust




Overview of the nQrux® Root of Trust hardware architecture.

## Introduction

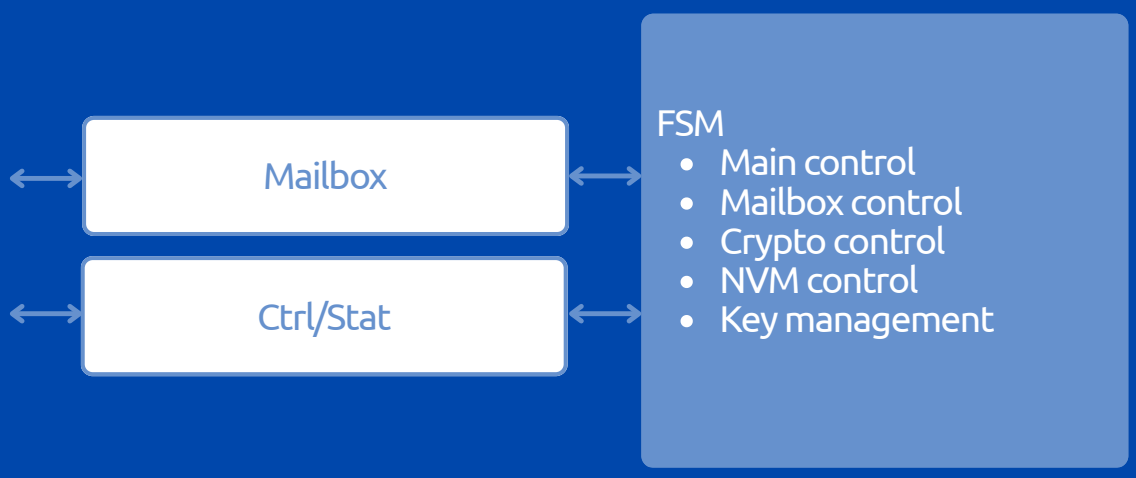
At the core of the nQrux® Root of Trust is a Finite State Machine (FSM) that coordinates security functions through dedicated hardware logic. The architecture brings together host communication, key and data protection, and cryptographic operations without requiring an embedded CPU or firmware.

The following sections explore these functions and how they work together within the Root of Trust.

# Secure communications

The nQrux® Root of Trust communicates with the host system through a 32-bit mailbox interface.

- Mailbox communication: Enables the exchange of commands and data between the host system and the Root of Trust.
- Protected communication:  AES256-GCM encryption and authentication help protect communication against eavesdropping and manipulation.
- Interface control: The FSM manages mailbox communication and coordinates access to internal security functions.

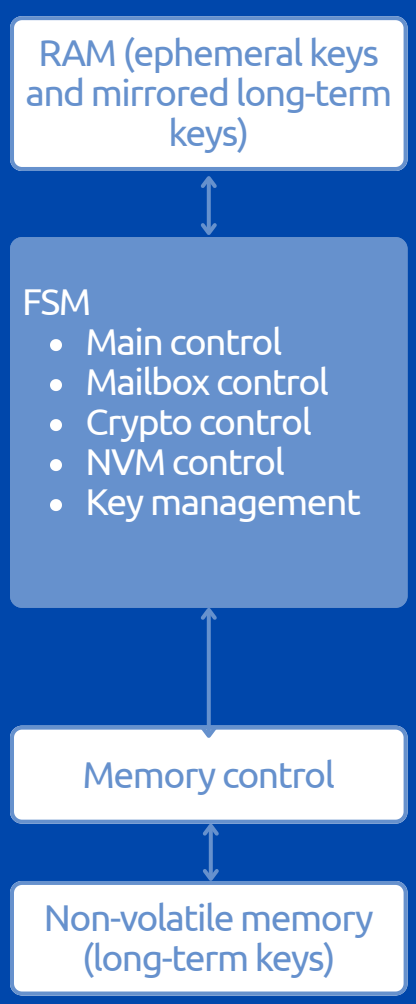



Mailbox and control/status interfaces connected to the FSM.

# Key and data protection

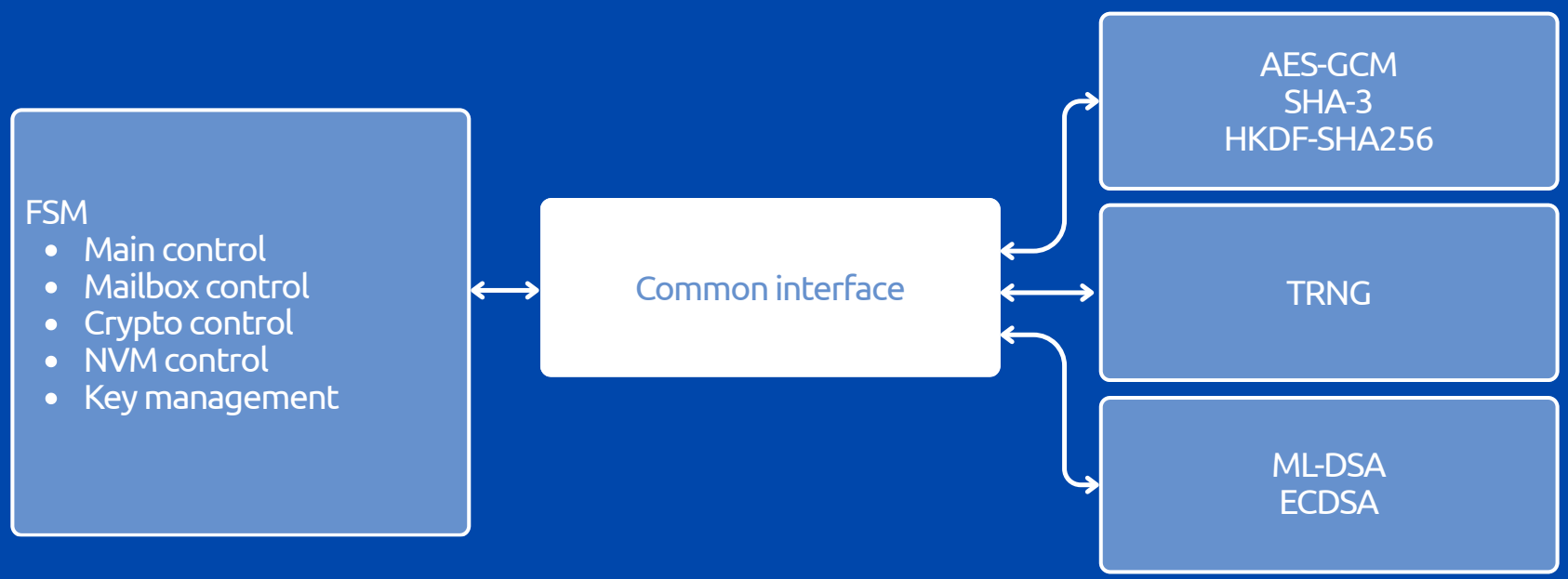
The architecture separates temporary and long-term key storage and controls access to cryptographic keys and data.

- Temporary key storage: RAM stores ephemeral keys and mirrored long-term keys.
- Long-term key storage: Non-volatile memory (NVM) provides persistent storage for long-term keys.
- Access control: User-specific memory spaces and defined permissions control access to keys and data.




*FSM-controlled access to RAM and non-volatile key storage.*

# Cryptographic operations




Cryptographic hardware modules connected to the FSM through a common interface.

The FSM coordinates cryptographic operations through a common interface connecting dedicated hardware modules.

- Cryptographic functions: AES-GCM, SHA-3 and HKDF-SHA256 support encryption, hashing and key derivation.
- Random number generation: A True Random Number Generator (TRNG) provides random numbers for cryptographic operations.
- Digital signatures: ECDSA and ML-DSA provide classical and quantum-resilient digital signature capabilities.

# Deterministic execution




FSM control functions for cryptographic operations, key management, mailbox communication and memory access.

The nQrux® Root of Trust uses a Finite State Machine (FSM) to coordinate security functions through predefined hardware-controlled state transitions.

- State-based control: The FSM manages cryptographic operations, key management, mailbox communication and memory access.
- Deterministic execution: Operations follow predefined execution sequences and state transitions.
- Firmware-free architecture: Dedicated hardware logic performs control functions without an embedded processor or firmware.

# nQrux® Root of Trust: Key design characteristics

### Firmware-free architecture
Pure RTL. No software stack to integrate, update or attack.

### Fast track to a secure foundation
Reduces development effort and lead times, allowing R&D to focus on product innovation.

### Post-quantum ready
Device identity built on hardware ML-DSA and ML-KEM.

### Smaller footprint on silicon
Hundreds of thousands rather than millions of gates in ASIC implementations.

### Low power
Less logic and memory means lower power consumption.

### Easy to integrate and retrofit
32-bit mailbox interface. FPGA, ASIC and SoC.

### Streamlined testing and verification
Simplified testing, validation, verification and certification processes.

# nQrux® Root of Trust

Learn more about its cryptographic capabilities, technical specifications and integration options.

XIPHERA

www.xiphera.com