XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP7450B: nQrux® Root of Trust

A Quantum-Resistant Hardware Root of Trust IP Core

Product Brief
ver. 1.0.0 September 25, 2026 sales@xiphera.com

Introduction

Root of trust is the component that can always be trusted in a computing system and acts as the trust anchor for building trust within the entire system. It must be immutable so that attackers cannot alter its contents or behavior. nQrux® Root of Trust stores cryptographic keys securely and uses them to perform a range of cryptographic operations. It manages, for example, trusted keys for verifying the authenticity of software and firmware during system boot. nQrux® Root of Trust is an IP core that implements a root of trust for a hardware system.

Key Features

- **Enabler for trusted computing:** nQrux® Root of Trust creates trust in a computing platform by providing a hardware root of trust for the system.
- **FSM based design:** The architecture of nQrux® Root of Trust is based on finite state machines implemented with pure digital logic without any hidden processors or software components, offering first-grade security with reduced complexity, simpler verification, smaller footprint, and lower power consumption.
- **Modern cryptography:** nQrux® Root of Trust supports a modern set of cryptographic algorithms including AES-GCM, elliptic curve cryptography, and SHA-3 as well as quantum-secure algorithms.
- **Secure bus:** The communication interface is protected with AES256-GCM authenticated encryption, securing the bus from eavesdropping, manipulation, and replays.
- **Advanced user policies:** nQrux® Root of Trust support multiple users with access only to their own keys and data.
- **Easy integration:** The simple 32-bit mailbox interface supports easy system integration.

Functionality

nQrux® Root of Trust provides secure key storage and key management as well as cryptographic services using those keys. The key storage is split to temporary storage, which is active only for a single user session, and persistent storage, which stores the long-term keys and other values even over power cycles. nQrux® Root of Trust also offers user segregation so that different users have access only their own keys and data. Each command and response to/from nQrux® Root of Trust is protected for both confidentiality and integrity with AES256-GCM authenticated encryption, preventing bus eavesdropping, manipulation of the communication, and replay attacks. nQrux® Root of Trust provides contemporary algorithms, such as AES, elliptic curve cryptography, and SHA-3, as well as quantum-resilient ones.

The amounts of both temporary and persistent memory are configurable with synthesis parameters and the amount of storage for each user can be configured when the user account is created in nQrux® Root of Trust, allowing customisation based on user needs.

In addition to the nQrux® Root of Trust IP core, a tamper-proof non-volatile memory is needed to implement the persistent storage. The contents of this memory are (optionally) encrypted.

Block Diagram

The internal high-level block diagram of nQrux® Root of Trust is depicted in Figure 1.

Interfaces

The external interfaces of nQrux® Root of Trust are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of nQrux® Root of Trust. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure, example simulation waveforms, and resource requirements.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. nQrux® Root of Trust can be shipped in a number of formats, including netlist, encrypted, obfuscated or plain text HDL source code. Additionally, compilation scripts, a testbench, and a detailed datasheet including an integration guide can be included depending on the target architecture.

Export Control

nQrux® Root of Trust protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of nQrux® Root of Trust is controlled by Council Regulation (EC) No 2021/821 and its subsequent changes.

nQrux® Root of Trust can be immediately shipped to all European Union member states, Australia, Canada, South Korea, Japan, New Zealand, Norway, Switzerland, United Kingdom, and the United States.

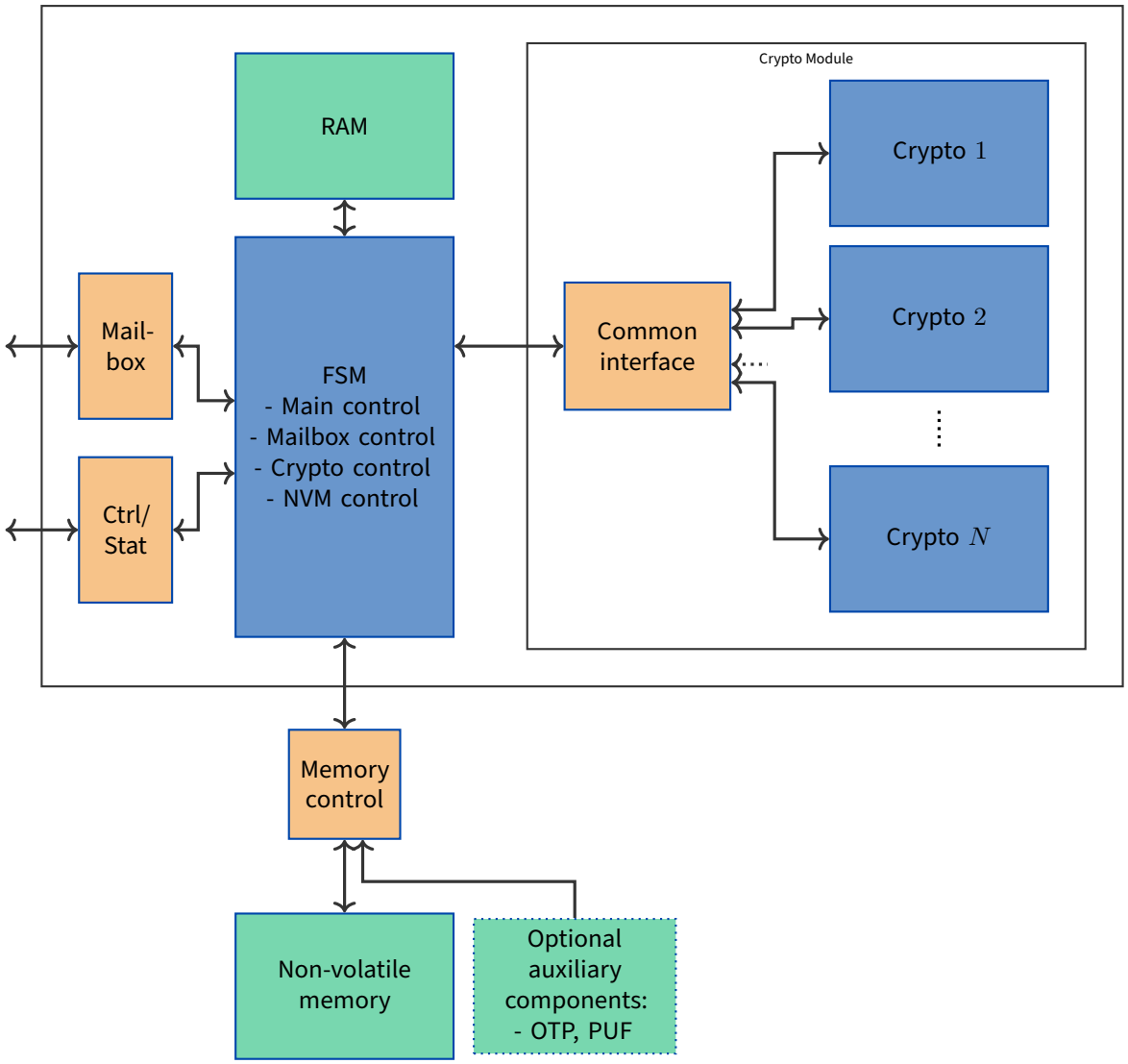


Figure 1: Internal high-level block diagram of nQrux® Root of Trust

Export to other countries requires authorization from The Ministry for Foreign Affairs of Finland, and a typical processing time for an export authorization is a few weeks.

About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Our fully in-house designed product portfolio includes individual cryptographic Intellectual Property (IP) cores, as well as comprehensive security solutions built from a combination of individual IP cores.

Xiphera is a Finnish company operating under the laws of the Republic of Finland, and is fully owned by Finnish citizens and institutional investors.

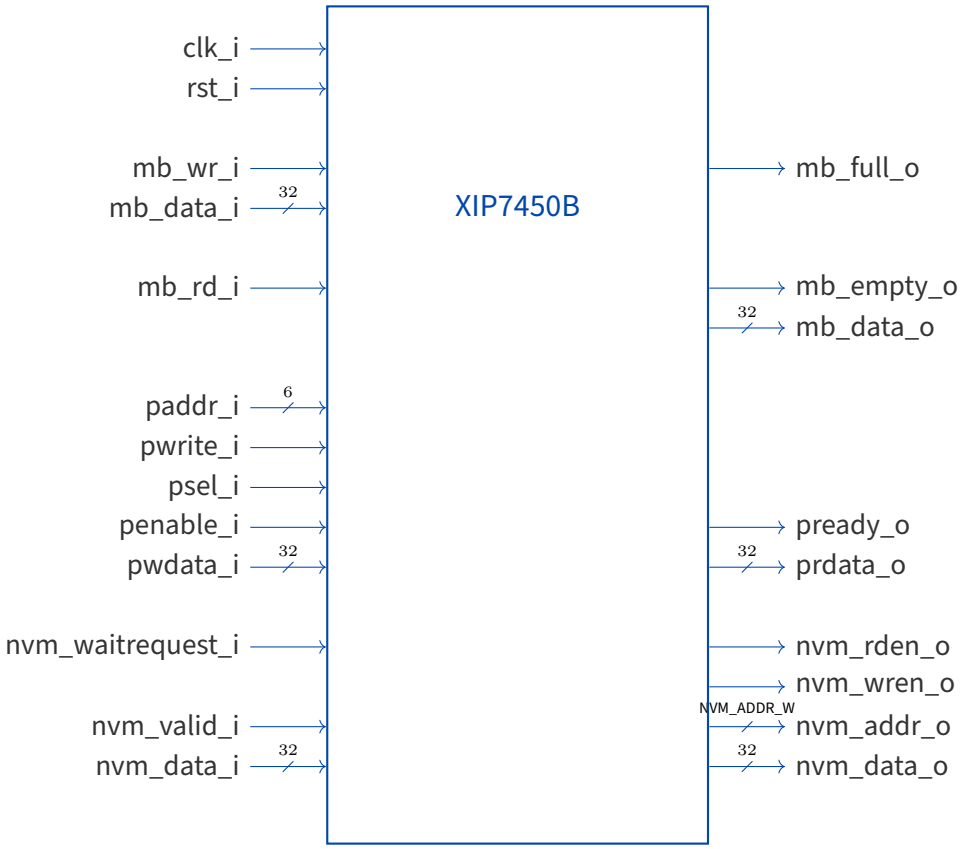


Figure 2: External interfaces of nQrux® Root of Trust

Contact

Xiphera Ltd.
Metsänpojankuja 1
FIN-02130 Espoo
Finland
sales@xiphera.com
+358 20 730 5252