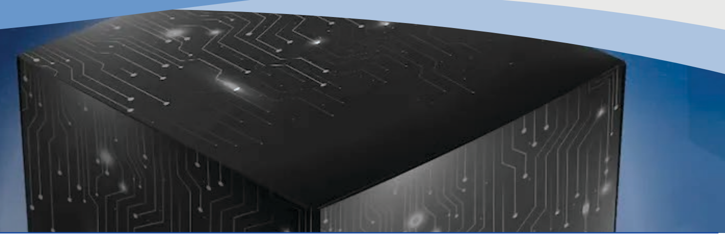
XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD



nQrux™ CCE

Confidential Computing Engine

Product code: XIP7700

nQrux™ Confidential Computing Engine (CCE) offers customisable solutions protecting data, code execution, and AI (Artificial Intelligence) models in distributed environments, such as cloud and edge. nQrux™ CCE solutions are tailored and optimised according to customer application, performance, and security requirements, to host customised computing resources (e.g. CPU cores and application-specific accelerators). Cryptographic algorithms are based on CAVP-verified implementations.

nQrux™ CCE securely processes data and code uploaded by client nodes over a TLS 1.3 protected communication channel. Clients can be categorised into groups with defined access rights to the resources hosted by the CCE. Access policies are enforced with hardware isolation of resources and TLS 1.3 client authentication.

KEY FEATURES

- Complete physical isolation of code & data
- Secure code & data transmission with TLS 1.3
- Quantum-safe crypto option
- Versatile computational enclave:
  - RISC-V or customer-specific cores
  - Application-specific accelerators
- Tailored based on application, security, and performance requirements
- Vendor agnostic FPGA implementation

APPLICATIONS

Tailored confidential computing infrastructures for:

- AI processing and remote code execution
- Remote use of accelerator IP cores in FPGA farms
- Data centers, edge, and cloud
- Space and satellite infrastructures
- Mission-critical applications
- Industrial and IoT environments

nQrux™ CCE

nQrux™ CCE is customised to meet customer application, performance, and security requirements.

SPECIFICATIONS

XIP7700

Secure code and data transmission

- TLS 1.3
  - AES256-GCM
  - SHA-384
  - ECDH(E)/ECDSA on NIST P-384

CPU

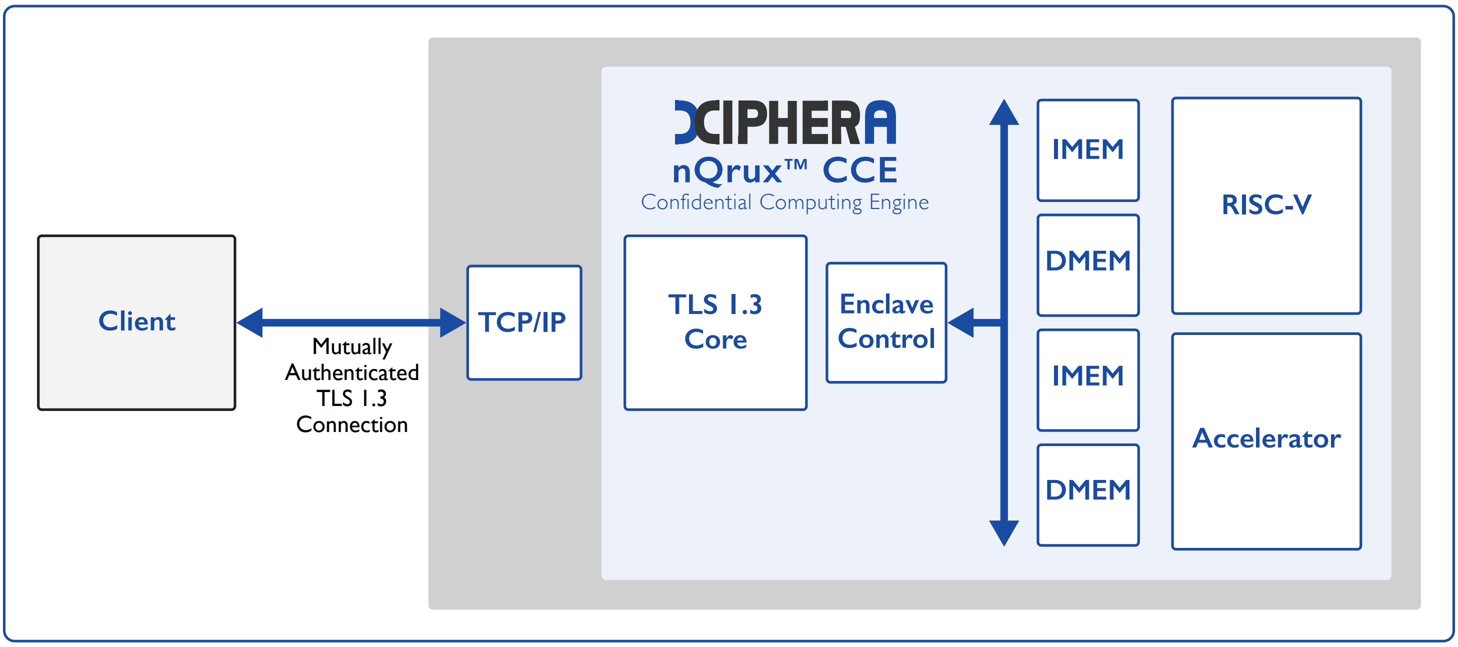
- RISC-V
- Optional customer-specific core

Accelerators

- Specified & implemented according to requirements

Post-Quantum Cryptography

- ML-KEM-512/768/1024 (CRYSTALS-Kyber)
- ML-DSA-44/65/87 (CRYSTALS-Dilithium)
- Implemented according to requirements



Deliverables

✓ Encrypted RTL or source code	✓ Optional netlist
✓ Sample synthesis scripts	✓ Instantiation file
✓ Comprehensive simulation test bench, scripts & guide	✓ Detailed datasheet and integration guide

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.

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

Tekniikantie 12
02150 Espoo
Finland

Email: sales@xiphera.com
Phone: +358 20 730 5252
Web: www.xiphera.com