Quantum Shield - QS7001

Quantum Resistant CCEAL5+ open RISC-V platform

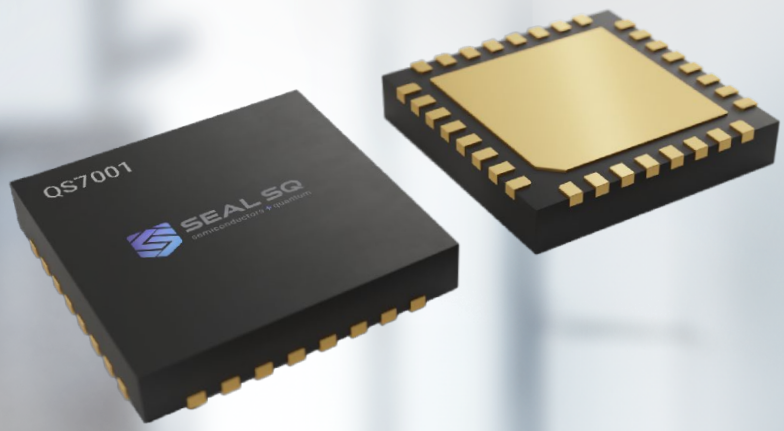
A powerful and versatile secure open platform with all the latest cryptographic algorithms, including quantum resistant NIST-appointed Kyber & Dilithium, to provide state-of-the-art security to a wide range of applications

Certified
Common Criteria EAL 5+ Hardware

Flexible
Load your firmware to power any kind of application

Quantum Resistant
NIST-appointed algorithms

Powerful
RISC-V CPU



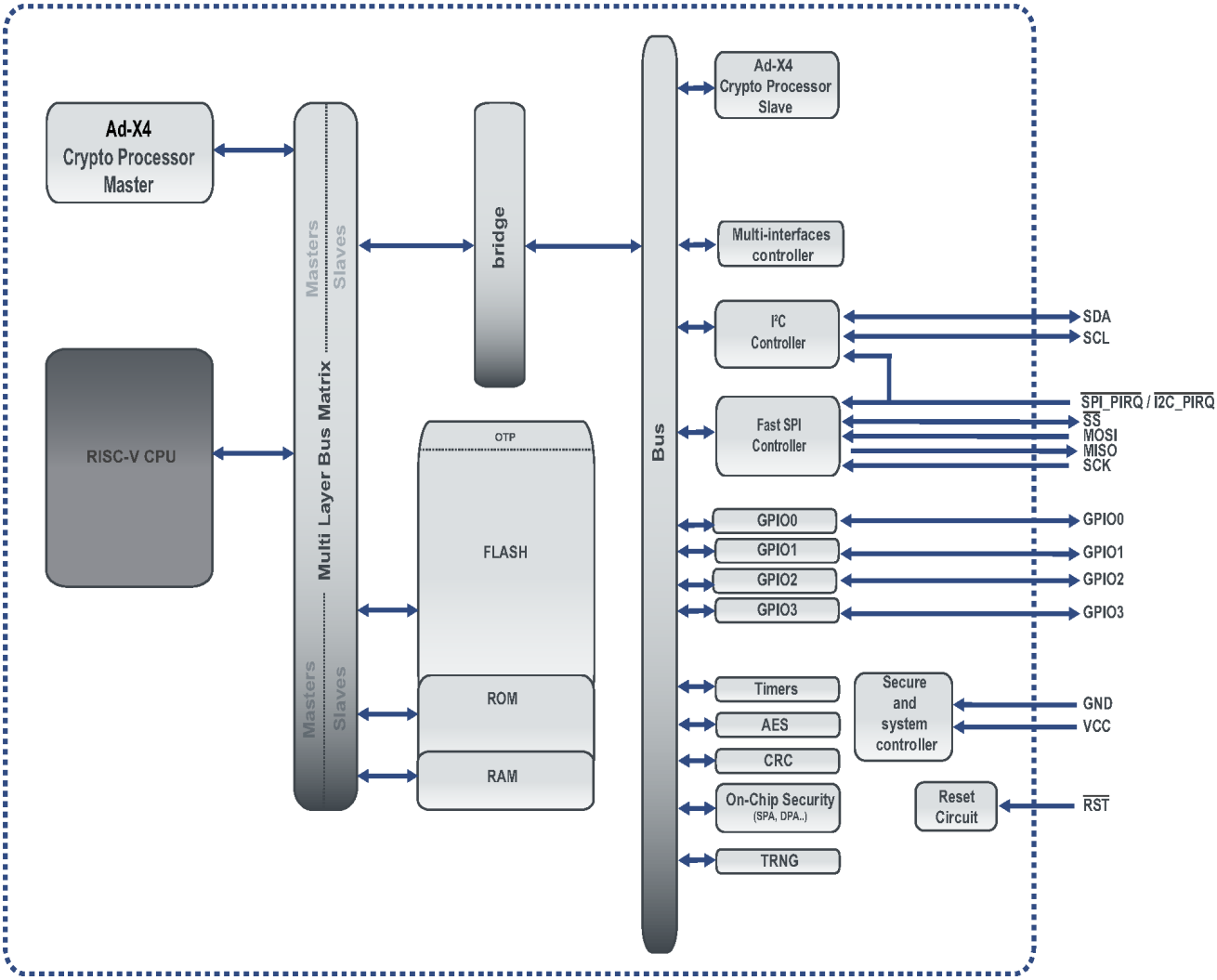
COMMON CRITERIA CERTIFIED EAL5+

FIPS 203
FIPS 204

NIST

RISC-V

Block Diagram Quantum Shield



Technical Features

- 80MHz 32-bit Secured RISC-V CPU
- 512KByte Flash, 80KB RAM, 4K executable RAM, 128k ROM (Crypto, Wear Leveling)
- 1Mbps I2C, 33MHz SPI (Communication Interface Auto Detect)
- 4 GPIOs
- 3 timers
- 64 bit unique Chip Serial Number
- Crypto accelerators (ECC, RSA, DH, CRC,...)
- RSA (up to 4096), ECC (256/384), AES (128/192/256), SHA2(256/384)-SHA3(256/384), NIST FIPS 203, 204
- 1.62V to 3.6V, -40°C to 105°C Operating Ranges
- QFN32 Package – TPM Compliant Pinout (I2C & SPI)