QS7001

Summary Datasheet

©SEALSQ - 2024 - All rights reserved

SEAL SQ
semiconductors + quantum

Features

General

- High-performance, Low-power 32 bits Secure RISC-V Architecture Microcontroller (Based upon Ibex/ETH platform)
- Internal Variable Frequency Oscillator up to 80 MHz
- Low Power Idle and Power-Down Modes
- ESD Protection up to ± 4000V
- Operating Range: 1,62V to 3,6V
- Operating Temperature: -40°C to +105°C
- Available in Wafers, standard ROHS packages

Packages

- 32-QFN (RoHS compliant)

Memory

- 512K Bytes of FLASH memory
  - 15 years data retention
  - 100k Write/Erase Cycles Native
  - Up to 500k Write/Erase Cycles using Wear-Leveling
- 80K Bytes of RAM Memory
  - 60K Bytes of RISC CPU RAM
  - 20K Bytes of Cryptographic Accelerator RAM (shared with the RISC CPU core)
- 4K of executable RAM as Cache
- 128K Bytes of ROM
  - Crypto Library
  - Wear-Leveling

Communication

- Slave SPI Serial Controller up to 33MBits/s
- Master SPI Serial Controller up to 20MBits/s
- I²C (Two Wire Interface) up to 1 Mbits/s

Peripherals

- Hardware Communication Interface Detection
- 4 GPIO
- 3 Timers
- 2-level Interrupt Controller
- Random Number Generator (RNG) SP800-90B compliant
- Hardware AES 128/192/256 Engine
- Checksum Accelerator
- CRC 16 & 32 Engine (Compliant with ISO / IEC 3309)
- 32-bit Cryptographic Accelerator
  - RSA, DSA, ECC, Diffie-Hellman, Key Generation
  - Post Quantum Cryptography: Crystal Kiber (KEM), Crystal Dilithium (Signature)

Security

- Dedicated Hardware for Protection Against SPA / DPA / SEMA / DEMA Attacks
- Advanced Protection Against Physical Attack, including Active Shield
- Environmental Protection Systems
  - Voltage Monitor
  - Frequency Monitor
  - Temperature Monitor
  - Light Protection
- Secure Memory Management/Access Protection (Supervisor Mode)

Certification Targeted

- CC EAL5+
- FIPS SP800-90B

6658ES – 20Dec24

Description

The QS7001 Architecture is based on SEALSQ's Secure RISC-V core which offers high performance and very low power consumption.

The QS7001 features a ROM memory dedicated to the storage of low-level drivers, wear leveling and cryptographic code.

A large flash memory mapped in both data and code space provides a flexible way to store user data and program code.

The ad-X4 hardware cryptographic accelerator featured in the QS7001 is dedicated to perform fast encryption or authentication functions, including crypto acceleration for post quantum cryptography.

Additional security features include fault injection resistance, hardware shield, scrambling of program, data and addresses, power analysis countermeasures and memory access controller by privileged modes.

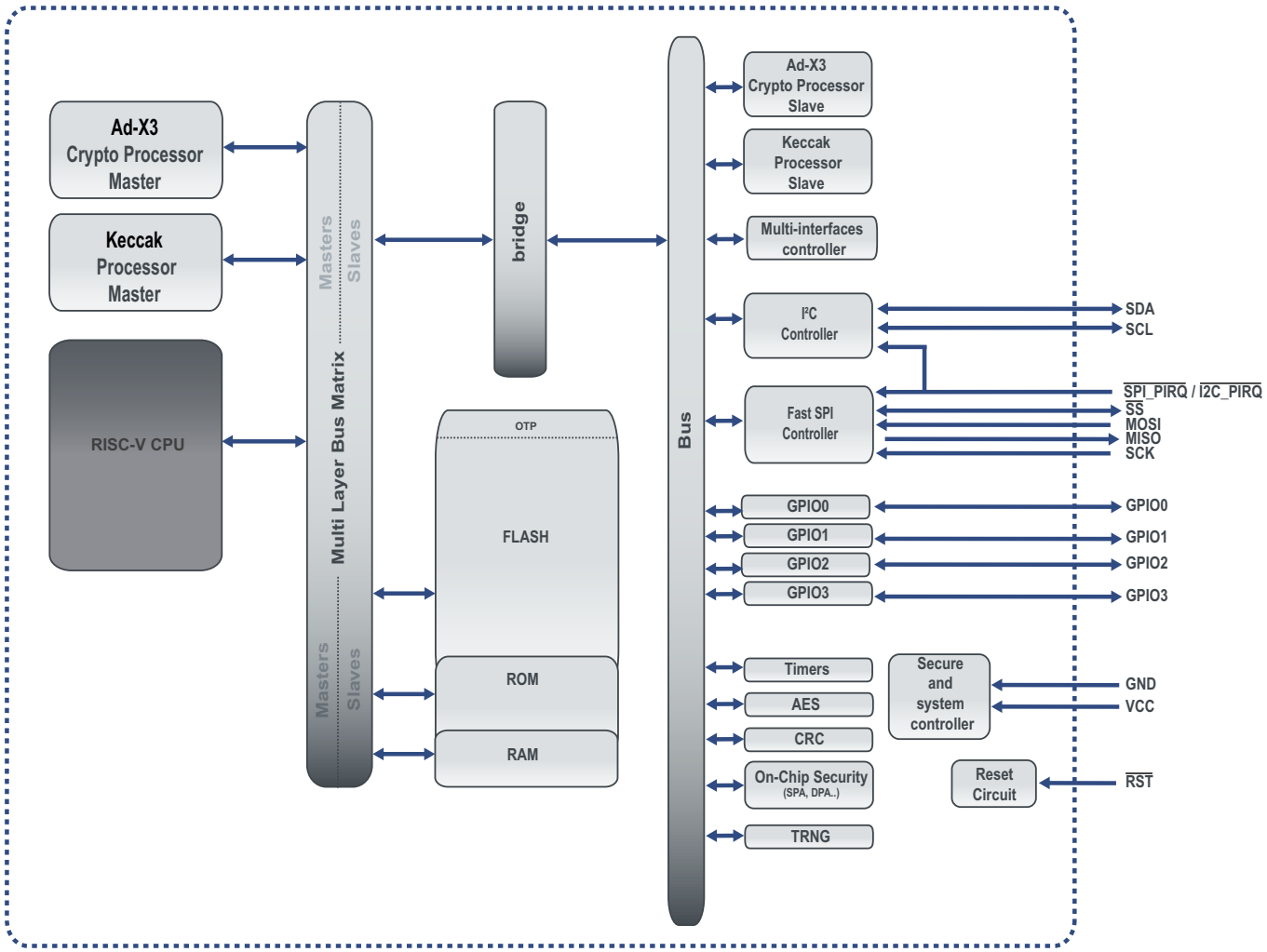
A DMA controller allows a fast transfer between the CPU RAM and the DPRAM banks. When configured as a master, the High-Speed SPI, provides a clock up to 20MHz thanks to the dedicated internal VFO clock system. The internal DPRAM memory provides 4 DPRAM buffers of 16 bytes each. The SPI controller features three sources of interrupt (Byte Transmitted, Time-out and Reception Overflow), a programmable clock and interbyte (guard time) delays.

The I²C interface interconnects components on a unique two-wire bus, made up of one clock line and one data line with speeds of up to 1Mbits per second, based on a byte-oriented transfer format. It is programmable as a master or a slave with sequential or single byte access. Multiple master capability is supported. Arbitration of the bus is performed internally and puts the I²C in slave mode automatically if the bus arbitration is lost.

Thanks to its dedicated set of peripherals, the QS7001 is an ideal product for applications such as Strong Authentication of Embedded Systems.

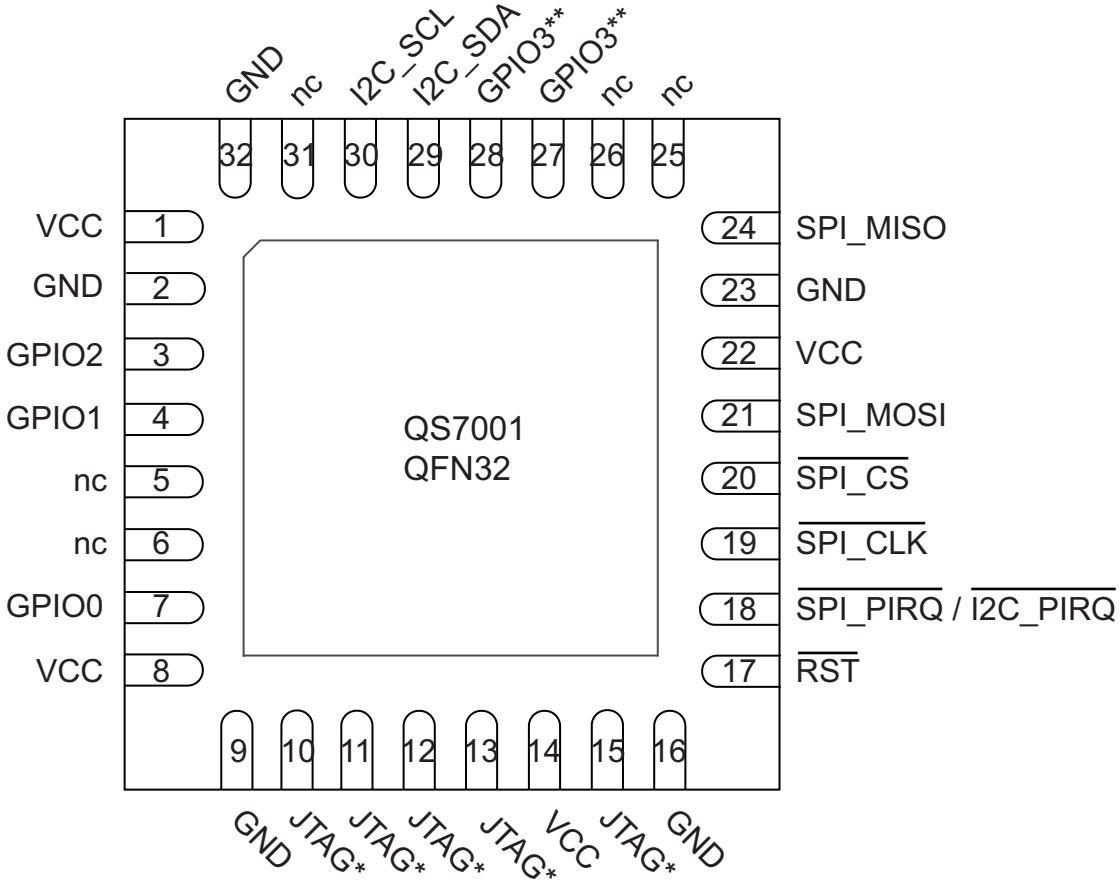
6658ES – 20Dec24

QS7001 Core Architecture



6658ES – 20Dec24

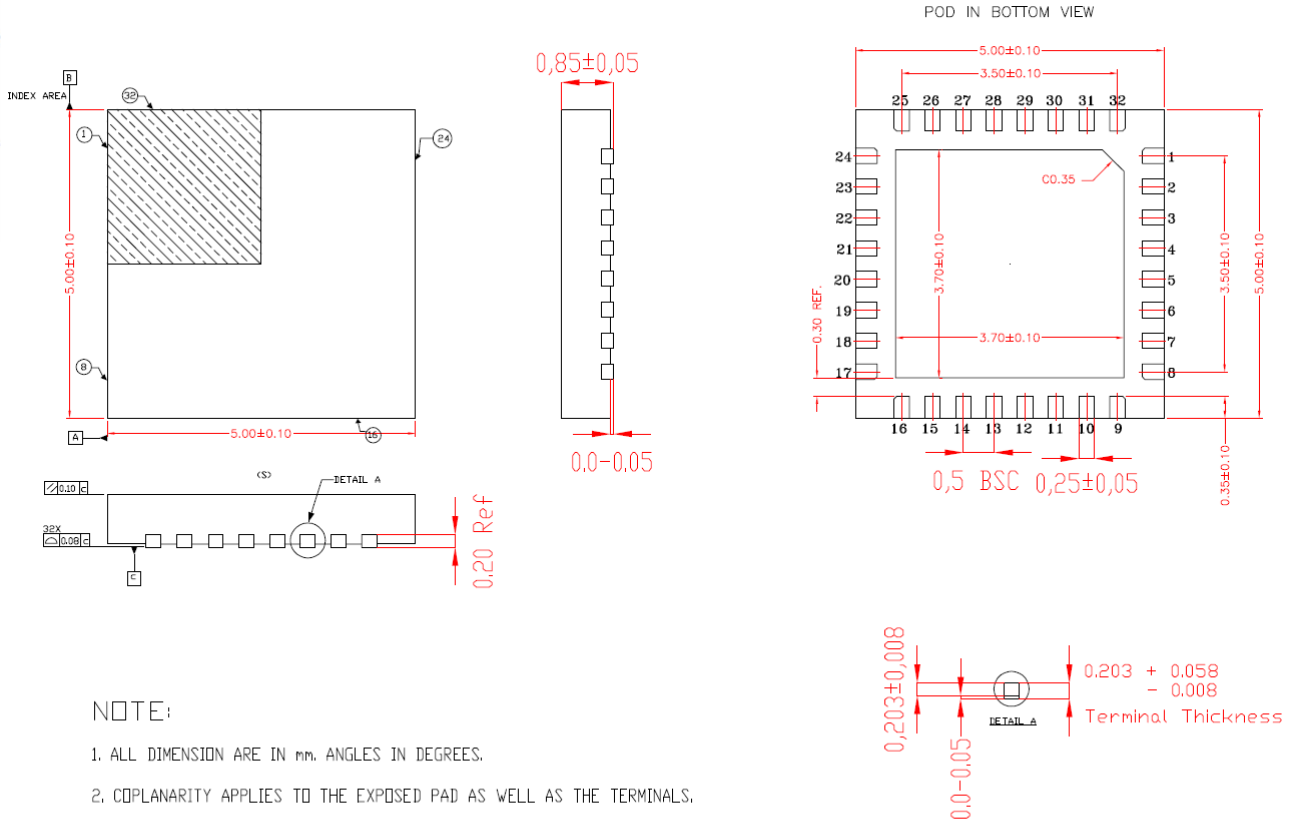
Pinout



nc = not internally connected
* JTAG is for devt. chips only
** double bonding of GPIO3

The exposed pad is not internally connected (floating).
It is recommended, but not mandatory, to connect it to the board GND

Package



NOTE:

1. ALL DIMENSION ARE IN mm. ANGLES IN DEGREES.
2. COPLANARITY APPLIES TO THE EXPOSED PAD AS WELL AS THE TERMINALS.
   COPLANARITY SHALL NOT EXCEED 0.08 mm.
3. WARPAGE SHALL NOT EXCEED 0.10 mm.
4. PACKAGE LENGHT / PACKAGE WIDTH ARE CONSIDERED AS SPECIAL CHARACREISTIC. (S)
5. REFER JEDEC MO-220

The photographs and information contained in this document are not contractual and may be changed without notice. Brand and product names may be registered trademarks or trademarks of their respective holders.
Note: This is a summary document. A complete document will be available under NDA. For more information, please contact your local Seal SQ sales office.