

Security Processor Based on 32-bit RISC Core

168MHz frequency, 128K SRAM, 4MB Flash, 2 × SmartCard, USB FS

Features

- 32-bit Processor
 - 32-bit RISC Core
 - MPU (Memory Protection Unit)
 - Operating frequency: 168/156/144/132/120/108/96 MHz (configurable via 1/2/4 frequency division)
- 1 secured JTAG-DP / SW-DP debug port
- 128KB randomly scrambled SRAM
- 1MB / 4MB Flash options
- System Control Module (manages clock gating for all peripherals and system-level configurations)
- Hardware Cryptographic Acceleration Engine
 - Symmetric algorithms: DES, TDES, AES-128/192/256
 - Asymmetric algorithms: RSA-1024/2048/4096, ECC 192~521
 - Hash algorithms: SHA-1/224/256/384/512, SHA3
 - Post-quantum cryptography (PQC) compliant algorithms: ML-KEM (FIPS 203), ML-DSA (FIPS 204)
- 2 SmartCard interfaces (compliant with EMV Level-1 and ISO7816-3 standards). SCIO integrates 7816 level shifter, which can be configured via registers to output 5V / 3V / 1.8V voltage levels.
- 3 UART interfaces (all support 4-wire mode)
- 3 SPI interfaces (1 configurable master/slave, 2 master-only)
- 1 high-speed SPI (HSPI) with master/slave configurable mode
- 1 I2C interface
- 6 × 32-bit Timers with PWM generation capability
- 1 True Random Number Generator (TRNG)
- 1 DMA controller with 4 independent DMA channels
- 1 CRC module (supports 16-bit / 32-bit CRC and multiple standard polynomial calculations)
- Tamper detection: supports 8 static tamper inputs or 4 groups of dynamic tamper inputs, configurable between static and dynamic mode
- Internal sensor array: monitors overvoltage / undervoltage, overtemperature / undertemperature, mesh tamper, clock anomaly and voltage glitch attacks
- Dedicated key storage area with hardware accelerated mass erase function
- 1 USB Full-Speed (FS) Device controller
- On-chip integrated watchdog timer
- 7-channel 10-bit ADC with maximum sampling rate up to 3.6 Msps, input voltage range: 0~1.2V or 0~3.6V
- On-chip magnetic stripe card decoder, compliant with ISO/ABA, AAMVA, IBM, JIS II and other card standards
- 7 independent power-domain GPIOs, operable at 1.8V or 3.3V
- Operating voltage: 2.7V ~ 3.6V
- Operating temperature range: -40°C ~ +85°C
- Package Type:
 - QFN88
 - BGA121