SECURE-iC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Crypto Solutions

CRYPTO SOLUTIONS neo CORE PLATFORM

The Crypto Solutions neo Core Platform embeds a hardware IP Crypto Coprocessor that accelerates cryptographic operations in System-on-Chip (SoC) environment on FPGA or ASIC.

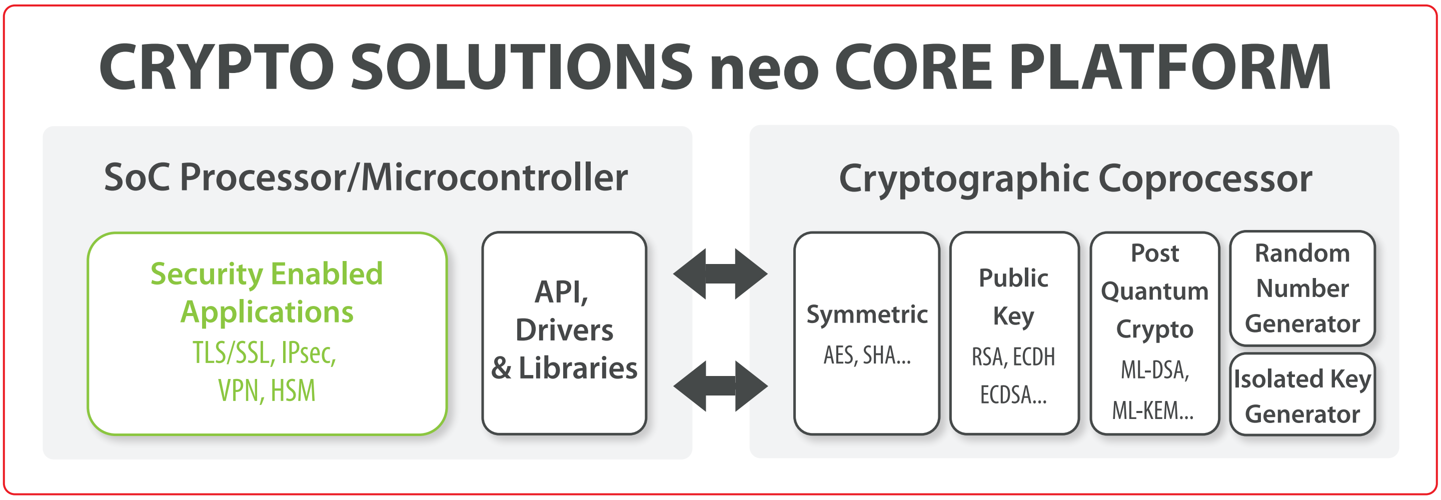
Symmetric operations are offloaded very efficiently as it has a built-in scatter/gather DMA. The coprocessors can be used to accelerate/offload IPsec, VPN, TLS/SSL, disk encryption, or any custom application requiring cryptography algorithms.

General description

The Crypto Solutions neo Core Platform integrates a selection of cryptographic IP cores (including TRNG solutions) following Customer needs. With interface, DMA and Software layers, it constitutes a complete solution.

The following cryptographic engines are available:

- Public Key Cryptography (RSA, ECC, ECDSA, ECDH,…)
- Random Number Generator (compliant with NIST-800-90A/B/C)
- AES (CTR, CCM, CMAC, GCM/GMAC, XTS, ECB, CBC, …)
- Hash: SHA-1/SHA-2/HMAC, SHA-3
- Chinese algorithms: SM2, SM3, SM4
- Chacha20-poly1305
- ARIA
- 3GPP security (ZUC, KASMI, SNOW_3G)
- DES and 3-DES (Ideal for legacy)
- PQC: ML-KEM, ML-DSA, SLH-DSA, FN-DSA, XMSS



CRYPTO SOLUTIONS neo CORE PLATFORM

SoC Processor/Microcontroller

Security Enabled Applications
TLS/SSL, IPsec, VPN, HSM

API, Drivers & Libraries

Cryptographic Coprocessor

Symmetric
AES, SHA...

Public Key
RSA, ECDH
ECDSA...

Post Quantum Crypto
ML-DSA,
ML-KEM...

Random Number Generator

Isolated Key Generator

Features

- ✓ Scalable architecture and crypto engines for optimal performance/resource usage
- ✓ Configurable for perfect application fit
- ✓ 100% CPU offload with low latency and high throughput
- ✓ Optional DPA countermeasures for AES, PK and SM4
- ✓ Can use keys (from PUF or others) hidden from CPU
- ✓ Software library integrated in MbedTLS3.x
- ✓ Full software/driver support
  - mbedTLS integration
  - OpenSSL support
  - Linux drivers (Crypto API integration)
- ✓ Easy integration
  - AHB/AXI interfaces
- ✓ FIPS 140-2 validated: CAVP #C742
- ✓ Low power

Applications

- ✓ Secure Communication (TLS, IPSec, BLE, Zigbee, others…)
- ✓ Secure boot support
- ✓ Secure storage
- ✓ Key generation

Software Interfacing

The software API and drivers are interfacing with mbedTLS and the CryptoAPI from the Linux OS. They are provided with the Crypto Solutions neo Core Platform to enable an easy integration with Customer application. Hardware offloading is directly available to applications using mbedTLs, OpenSSL or interfacing with the kernel through Cryptodev and AF_ALG.

Deliverables

- ✓ Netlist or RTL
- ✓ SW drivers (Linux) & OpenSSL
- ✓ Scripts for implementations
- ✓ Self-checking RTL test-bench based on FIPS vectors
- ✓ Documentation

Markets

- WIRELESS COMMUNICATION
- NETWORKING
- AUTOMOTIVE & SMART MOBILITY
- GENERAL PURPOSE MCU/MPU
- SERVER & CLOUD

Crypto Coprocessors

Offloads the intensive tasks from the main processor, increasing the system performance.

	COMPACT	STANDARD	HIGH-PERF	HIGH-SECURITY
	Specifically designed for devices with strict power & area constraints	Integrates TRNG and PKC IP cores, and SCA countermeasures	Support High-Performance implementations of AES-GCM, XTS	Support isolated hardware key generation & usage
Configurable for perfect application fit	✓	✓	✓	✓
100% CPU offload with low latency and high throughput	✓	✓	✓	✓
Full software/driver support	✓	✓	✓	✓
FIPS 140-2 validated: CAVP #C742	✓	✓	✓	✓
Secure boot support	✓	✓	✓	✓
Traditional Cryptographic Algorithms	AES, SHA/HMAC	AES, SHA/HMAC, PKC	AES (High-perf), SHA/HMAC, PKC	AES, SHA/HMAC, PKC
Chinese Cryptographic Algorithms (option)	SM4, SM3	SM4, SM3 SM2	SM4, SM3 SM2	SM4, SM3 SM2
Post-Quantum Cryptographic Algorithms (option)	✓	✓	✓	✓
SCA countermeasures on Cryptographic Algorithms	—	✓	✓	✓
True Random Number Generator (TRNG)	—	✓	✓	✓
Interfaces	AHB/AXI	AHB/AXI	AXI	AHB/AXI
Hidden asymmetric keys (attestation)	—	—	—	✓
Hardware key generation (hidden from CPU)	—	—	—	✓
Power/area	Very low	Low	High	Medium
All variants offer full security features, and the same crypto engines can be included in all.	PRODUCT CODE SCZ_CS_S10_neo	PRODUCT CODE SCZ_CS_S30_neo	PRODUCT CODE SCZ_CS_S80_neo	PRODUCT CODE SCZ_CS_S90_neo

V4.0

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US
www.secure-ic.com