Crypto & Security Solutions

From IP to fully integrated system

Security IP Platforms & Solutions

- eSecure Embedded Security module
- HW Root of Trust
- Secure boot and secure storage
- Cryptographic Coprocessor for SoC
- IPsec and MACsec high throughput engines
- TLS/SSL connection engine
- Bus encryption/protection

Cryptographic IP cores

- Asymmetric algorithms
  - RSA, CRT, DH, DSA up to 4096 bits
  - ECC/ECDSA/ECDH in F(p) and F(2m) up to 1024 bits
  - NIST, Brainpool, Koblitz and other curves
  - Curve25519, EdDSA, SRP for Apple Homekit
  - Rabin-Miller, primality check and key generation
  - J-PAKE, EC-KCDSA, ECIES, ECMQV
  - SM2
- Symmetric algorithms
  - AES multi-purpose (ECB, CBC, CTR, XTS, CCM/CMAC, GCM/GMAC, OFB, CFB)
  - High performance AES-GCM/CTR/XTS
  - Chacha20/Poly1305
  - SM4
  - Hashing (SHA-1, SHA-2, SHA-3, HMAC, MD5, SM3)
  - DES and 3-DES core
- Random Number Generators
  - TRNG (NIST800-90B and AIS-31)
  - DRBG (NIST800-90A compliant)
- Optimized for latest ASIC and FPGA technologies
- Best power, performance and area trade-off for any application

Silex Insight provides hardware solutions for cryptography and security based on FPGA, ASIC and SoC.

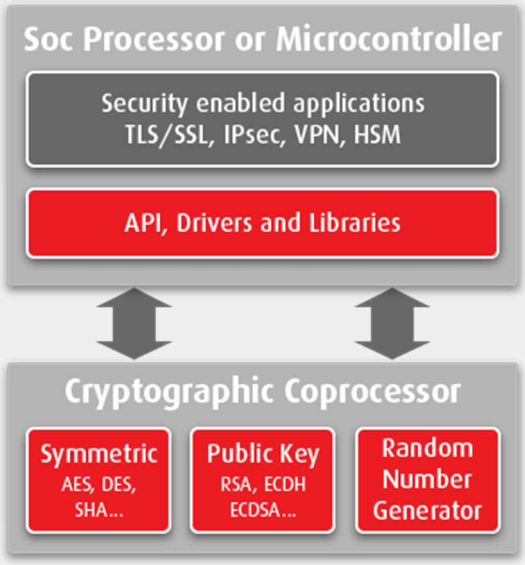
Cryptography is mainly used in applications requiring secure communications and storage of information. Therefore, our solutions are used in a wide variety of market segments including Internet of Things, wearables, industry 4.0, automotive, healthcare, payment, telecommunications and others. Silex Insight has a comprehensive set of security IP cores and platforms to address these markets.

The Silex Insight security **solutions, a combination of software and hardware,** provide the necessary security for your FPGA or ASIC design including secure boot, secure storage, and cryptographic operations co-processing.

Silex Insight provides solutions such as:

- HW Root of Trust
- Secure boot
- Secure storage
- Cryptographic Coprocessor
- Linux CryptoAPI and TLS/SSL acceleration

The Silex Insight silicon proven **IP cores** support symmetric and asymmetric cryptography. They are valued by the market for their worlds' leading ultra-high speed performance and compact footprint. Our IP cores are delivered with software drivers in order to be easily integrated in your system.



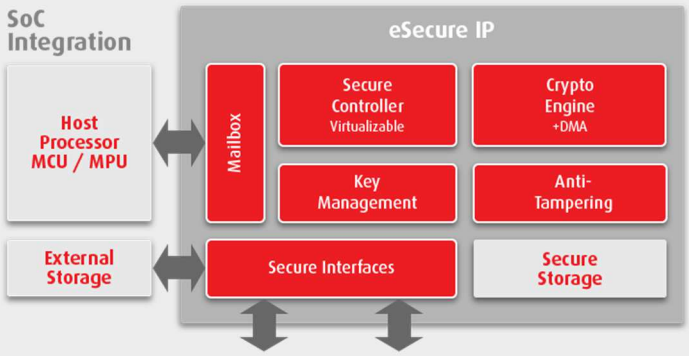
Crypto & Security Solutions

From IP to fully integrated system

eSecure IP module

The eSecure module is a complete solution to secure your ASIC or FPGA design. It is made up of hardware IP cores and software libraries that together will enable the security and cryptography required by your application:

- HW Root of trust
- Software/Firmware authentication (secure boot)
- Secure storage (keys, secrets, …)
- Secure firmware update in the field
- PF integration
- Secure debugging
- Anti-tampering
- Cryptographic operations off-loading



Optimized performance, power and area

The eSecure module is tailored to your application and will include all the necessary cryptographic operations. The cryptographic algorithms are implemented in hardware logic by using our silicon proven IP cores and enabling 100% offloading of the CPU. Each hardware IP core is flexible and scalable in terms of features and performance giving the best trade-off between performance, power and area.

Wide range of algorithms

The eSecure module integrates many different cryptographic algorithms in order to support several communication protocols and security schemes. The module is ready to support the latest protocols of the Internet of Things applications such as TLS/DTLS 1.3, Apple HomeKit, Thread networking.

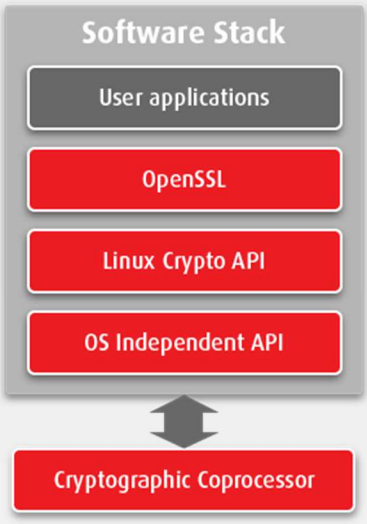
Suitable for all applications

Thanks to the efficiency of the hardware and the flexibility of the software. The module can be used to address all sort of applications. It can be used for low power or high performance systems to secure communication, device and storage.

Full software stack for Linux operating system

For applications running on top of Linux, whether on FPGA SoC devices or custom ASIC, the platform is provided with a full software solution for easy integration. The aim is to provide transparent access to the efficient hardware cryptographic implementations by using standard software libraries.

Linux Kernel drivers are provided to enable the cryptographic coprocessor in the Linux CryptoAPI. This integration, for example, enables the efficient use of the IPsec networking protocol. The engine for OpenSSL enables the offloading of the cryptographic functions for applications based on this library.



SILEX INSIGHT

Crypto & Security Solutions

From IP to fully integrated system

Standalone cryptographic IP cores

Public Key engine (BA414EP)

The Public Key engine has a µCode based architecture that can support several algorithms and operations, allowing to completely (100%) offload the CPU. This architecture gives the efficiency of the hardware and the flexibility of the software. The flexibility and scalability of the Public Key engine enables us to have the best-in-class performance/resources ratio.

Supported operations:

- RSA (up to 8192 bits), DSA, CRT, DH
- ECC (up to 571 bits), DSA/ECDSA, F(p) and F(2m)
- Curve25519, EdDSA, SRP (Apple HomeKit), SM2
- J-PAKE, EC-KCDSA, ECIES, ECMQV
- Rabin Miller, primality check, key generation

Random Number Generator (BA431)

The random number generator is an essential part of all secure systems. Silex Insight provides a True Random Number Generator (TRNG) and a Deterministic Random Bit Generator (DRBG).

Features:

- TRNG compliant with NIST800-22 and AIS-31 test suite
- TRNG compliant with NIST800-90B (health tests and conditioning)
- DRBG compliant with NIST800-90A (Hash_DRBG or AES_DRBG)
- Linux driver and OpenSSL integration

Hash engine (BA413)

Our Hash core supports several hashing algorithm widely used in cryptography world. The hash core is especially used for data integrity verification, authentication and secure boot.

Hashing modes: SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3 HMAC, SM3 and MD5.

CHACHA20-POLY1305 (BA417)

The BA417 IP core is a RFC7539 compliant crypto engine to provide Authenticated Encryption with Associated Data (AEAD) using the Chacha20 stream cipher combined with the Poly1305 message-authentication code. It has simple interfaces and is easy to integrate.

High Performance AES-GCM/XTS/CTR

The AES-GCM/XTS/CTR IP core provides high speed AES encryption and authentication. The IP core is scalable, and can be configured to reach the bandwidth needed (up to 100Gbps).

Crypto & Security Solutions

From IP to fully integrated system

Electronic Design Services

- ASIC
- FPGA
- DSP
- Software
- Board/system

Video over IP reference design

- SD/HD/3G-SDI, Gigabit Ethernet, 10GbE
- JPEG 2000 compressed or uncompressed
- MPEG-2 TS
- SMPTE2022-1,2,5,6 with FEC
- Xilinx 7 series FPGA's & Zynq SoC
- VSF interoperable profile for broadcast

Video Platforms

- Video in/out (SDI/HDMI/Display Port/ DVB ASI/PCIe...)
- Processing (rotation, scaling, interlacing, noise reduction, image dithering…)
- JPEG 2000 compression
- Transport (SMPTE2022/Ethernet AVB/RTP)
- Network streaming
- High efficiency memory controllers

Video compression IP cores

- JPEG 2000
- VC-2 LD
- JPEG
- MPEG-2

Security Platforms

- eSecure
- Cryptographic co-processor
- IPsec/MACsec engine
- TLS/SSL connection engine
- Bus encryption/protection

Cryptographic IP cores

- Public Key engine (RSA, ECC, …)
- AES Flex engine (ECB, CTR, CBC/CMAC, OFB, CFB)
- AES GCM (MACsec, IPsec…)
- AES XTS (disc storage …)
- CHACHA20-POLY1305
- Hash core (SHA-1, SHA-2, SHA-3, HMAC, MD5)
- TRNG, DRBG (NIST800-90 compliant)

Silex Insight provides **image processing** and **security** solutions as well as **electronic design** services (ASIC, FPGA, DSP, embedded software, Board).

Silex Insight can interact at different stages in the development cycle of your products: from providing IP cores, reference designs and platforms, support on part of your integrated design to the delivery of a full turnkey solution.

The unique combination of Silex Insight's image processing expertise and top-notch **electronic design** skills enabled many customers to accelerate their video product developments with leading-edge and cost-effective solutions. We are recognized for our state-of-the-art expertise in complex and high-speed design, for our project management skills and for our reliable design methodology.

Silex Insight's **video platforms** and **reference designs** integrate a full-range of compression and networking modules. They benefit equipment OEM's who need to accelerate the development of video solutions that can adapt to changes in critical standards, specifications and protocols. Our Video-over-IP reference design integrates the latest video over IP capabilities (SDI, SMPTE2022, JPEG 2000, MPEG-2 TS, 1&10Gb Ethernet).