Securing platforms at their heart to offer cost-optimized and low power solutions

Hardware and software solutions must be combined to provide best-in-class protection and deliver quick time-to-market while reducing design cost.

www.insidesecure.com
The growing demand for a connected environment with rich end-user experience opens new market opportunities for the digital industry. As security challenges and threats continue to make headlines in our connected world, cars, but also lighting systems, mobile, smartwatches, white goods, home security devices, medical equipment, airplanes and industrial automation systems have all been vulnerable to cyber security attacks.

Today, Semiconductor makers, FPGA providers and device makers are accelerating the adoption of proven security solutions, making smart decisions that lead to an optimal balance between security, cost and performance. Building a secure SoC or ASIC requires an architecture crafted specifically for the types of threats these devices will be exposed to. These highly connected devices provide broad attack surfaces for hackers to exploit. To secure these devices, designers need a comprehensive security IP framework that provides the right level of security with the right functions in these devices as well as the best security software tools to increase quickly the security of the existing platforms.

As each use case have specific constraints (power consumption, spec, environment...) and can impose different security requirements (certifications to meet regulatory requirements, for example), the following functionalities will be important for the choice of the security solution to integrate:

- **Secure Identification/Authentication:** Verifying the identity of the communicating peer
- **Secure Communication:** Maintaining the confidentiality and integrity of communications between peers
- **Secure Data Storage:** Protecting data at rest
- **Platform Integrity:** Executing only trusted software at boot and during updates

The basis of those functions can be addressed with smart implementation of modern standard cryptography and associated services to manage the keys and digital certificates.
Inside Secure® delivers a comprehensive set of hardware and software products that can be combined to perfectly match application needs in terms of security, power consumption, speed and flexibility of implementation.

**SILICON IP CORES PRODUCTS**

**FUNCTIONS**
- Hardware Root-of Trust
- Secure key storage
- Secure execution of crypto functions (AES, SHA2-3, RSA, ECC, ...)
- True random number generator (FIPS certified)
- Side channels protection and anti-tampering

**KEY BENEFITS**
- Strong security against software and physical attacks (FIPS 140-2 Level 2 certified)
- Low power implementation
- Low area/gate count starting at 85K gates
- High throughput
- Silicon proven, delivered as portable & synthesizable RTL

**GUARD TOOLKIT PRODUCTS**

**FUNCTIONS**
- Secure communications (IPSEC, TLS/DTLS AND MACsec)
- Secure data storage (crypto keys, credentials, etc.)
- Secure execution of crypto functions
- Secure boot and software upgrade

**KEY BENEFITS**
- Reduce development cost
- Accelerate time-to-market
- Widely deployed software stacks used by major companies
- Highly portable well-documented and GPL-free ANSI C source code
- Interoperability tested, compliant to IETF and IEEE standards
- FIPS140-2 certified cryptography available
Silicon Security IP

Inside Secure proposes the largest silicon-proven security IP portfolio for next-generation system-on-a-chip (SoC) and application specific integrated circuit (ASIC) designs for High Speed Networking, Internet of Things, Datacenters and Content Protection, delivering quick time-to-market while reducing design cost.

Packet Engines for IPSec, TLS & SSL:
Unlike simple crypto-only accelerators, intelligent packet engines contain complete protocol knowledge, delivering the benefits of throughput acceleration and CPU offload. Intelligent Packet Engine IP offers acceleration of IPSec, MACsec, SSL/TLS/DTLS, sRTP and basic hash & crypto operations at target speeds ranging from 100Mbps to 100Gbps and beyond, in architectures ranging from the traditional look-aside engines to the more sophisticated, powerful inline packet engines.

Packet Engines for MACsec:
A complete solution comprising of a family of MACsec Security IP and a MACsec software toolkit targeting Data Center WAN routers and TOR switch, Access Providers Network interface devices, IP phones, switches, bridges, and routers for Layer 2 LAN and Metro Ethernet communications. Build Ethernet switch fabrics and PHY devices using MACsec IP engines to reach speeds from 1Gbps, 10Gbps, 100Gbps, 400Gbps and beyond. The IP provides a complete and standard compliant MACsec solution optionally supporting full Cisco ClearTags, which ensures auditable compliance while reducing development cost and time to market.

Cryptographic Accelerators:
Inside Secure’s cryptographic algorithm accelerator IP cores are standalone hardware IP cores for accelerating various symmetric, asymmetric ciphers, HASH and HMAC-based integrity algorithms, as well as true random number generators (TRNG).

Inside Secure’s Hash and HMAC accelerator IP cores are standalone hardware IP cores for accelerating various HASH and HMAC-based integrity algorithms. These cores are also embedded in packet engines as well as Vault-IP products.

Inside Secure’s cipher accelerator IP cores are standalone hardware IP cores for accelerating various symmetric and asymmetric cryptographic primitive algorithms. These cores are also embedded in packet engines as well as Vault-IP products.
Vault-IP Platform Security Solutions

Vault-IP is a family of security modules protecting the SoC platform, its identity and operations, so it can securely boot and protect sensitive key material and assets. It provides secure, energy-efficient accelerated security functions. Vault-IP has cryptographic and security functions on board to build trusted solutions, it includes a rich set of cryptographic services that are executed independently from the general purpose computing.

Two physical domains are created inside the SoC, the “non-secure” domain and the “secure” domain. Each domain runs independently of each other. The secure domain manages all sensitive tasks (e.g. crypto functions and secure storage) and can only be accessed through a firewalled interface.

The Vault-IP Secure Platform provides cryptographic building blocks (symmetric, asymmetric, hashing and true random number generation), as well as ‘trust anchors’ in hardware, allowing designers to implement a comprehensive security architecture without getting bogged down in the complexities of low-level cryptographic operation and key management.

The platform components provide a cost-efficient, low power and small footprint IP solution for system and platform integrity, and cryptographic acceleration services to applications.

The key attributes of the Vault-IP Secure Platform are secure boot, secure storage, secure debug, hardware Root of Trust, secure communication, and a secure asset store. Inside Secure’s Vault-IP can be delivered as a FIPS-certified silicon IP security module that easily integrates into any chip.

Vault-IP is a family of solutions, comprised of:

- **VaultIP-120**, a lightweight platform protections core, offering secure asset store, TRNG, ECC, AES, SHA-256, targeting single core closed designs
- **VaultIP-130**, providing extended functions, offering secure asset store, TRNG, RSA, ECC, AES, 3DES, SHA-1, SHA-256, SHA-512, targeting multi core Trustzone and non Trustzone designs
- **VaultIP-140**, providing additional algorithms on top of VaultIP-130, such as Poly1305, ChaCha2 and Curve25519, targeting Homekit and other IoT ecosystems.

---

*Caption: Example of a system diagram for Vault-IP-140*
GUARD PRODUCT FAMILY TO SECURE DATA & COMMUNICATION

The Guard product family inherits a long experience in cryptography and secure communication built for over 20 years under companies such as SSH technologies, SafeNet, AuthenTec and now Inside Secure. It leverages widely deployed products previously name QuickSec IPsec Toolkit, MatrixSSL or SafeZone FIPS cryptographic module with a focus on three markets.

All products are delivered as GPL free, C source code implementation to help customers build and maintain world class security in their products in a cost effective way. They are found in large scale gateways as in tiny IoT devices, and used to fulfill carriers, government or enterprise needs.

IoT and Embedded Security

GUARD embedded IoT security framework is a modular solution allowing IoT device and platform makers to deploy the security they really need.

A common API provides the needed cryptographic and certificates tools. Applications may choose FIPS140-2-certified, cryptography, hardware-based security or standard cryptography, depending on their needs. GUARD Secure Boot protects the core of the device.
A rich set of security protocols (TLS, DTLS, IPsec, MACsec) are available for IoT devices and embedded deployments.

Mobile Device Security
Helped by a growing set of hacking tools, criminals are targeting mobile devices more than ever to access valuable data, threatening user privacy and confidential information.

Common vectors of attack may be another computer using the same Wi-Fi, a compromised wireless router or a rogue access point. To protect against malware injection or data theft, mobile devices should systematically use a VPN, especially over untrusted Wi-Fi.

Our solutions rely on FIPS140-2-validated cryptography to protect the data through device encryption and IPsec VPN.

Clouds and secure communication
With more and more data residing in clouds, secure communication is more critical than ever. It protects privacy and data by ensuring confidentiality and integrity of the communication.

It also provides sender authentication that ensures that traffic is coming from a trusted peer, automatically discarding malicious data.

In particular, secure VPN must be used to access security functions deployed in clouds (security as a service) to prevent malware to be injected by local attack (e.g. fake Access Point).

A rich set of security protocols (TLS, DTLS, IPsec, MACsec) are available for cloud deployments.
Inside Secure® has demonstrated success in the personalization of integrated circuits for smart card application. Based on this experience, Inside Secure® can recommend services that will help customers manage security at any point during the device manufacturing chain from design to delivery to the end user.

For further details on all of Inside’s security solutions, visit www.insidesecure.com