



GAIA

A New Vision of Security on Silicon

Contact us

Headquarters

STARCHIP® SAS
Les Carrés de l'Arc
Bâtiment C
Rond-Point du Canet
13590 MEYREUIL
Tel. : +33 (0)4 42 26 45 77

Sales Office

STARCHIP®
Residence Parkile
Bâtiment 5
164, Avenue Joseph Kessel
78960 VOISIN LE BRETONNEUX
Tel.: +33 (0)1 34 52 20 75

Multimedia Support

Contact Press Relations : press@starchip-ic.com
Contact Investors : investors@starchip-ic.com

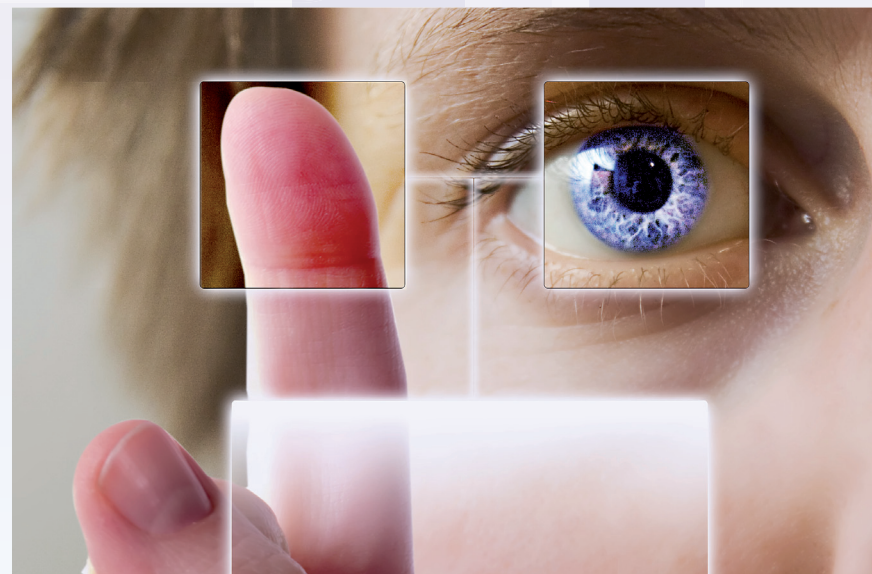
On Line Support

Contact Technical Support : support@starchip-ic.com
Contact Sales & Marketing Support : sales@starchip-ic.com

About StarChip®

StarChip® is a dynamic semiconductor company that enables customers to directly benefit from its unique, optimized value chain system. We design and qualify products for mass production, then license our solutions for purchase directly by our customers through qualified foundries and test houses.

StarChip® products are based on state-of-the art, flash-based 32-bit architectures. They are designed to offer maximum integration, providing support for embedded, innovative security technologies, analog functionality, and connectivity and control interfaces. The result is a flexible set of solutions that can easily meet the requirements of a wide variety of markets, including smart card and security, consumer, automotive, and industrial applications.



GAIA, the “Goddess of the Earth” from Greek mythology, is a philosophy of treating the Earth as a living, self-healing organism. At StarChip®, we apply this self-regulating view to our security architecture, integrating robust security mechanisms directly into the chip. The result is comprehensive, in-depth protection against a broad range of security risks, to help safeguard critical data and minimize recovery time. GAIA is an innovative, global vision for security on silicon

www.starchip-ic.com





GAIA: GLOBAL AUTO IMMUNE ARCHITECTURE

ASSESSMENT

StarChip® employs a skilled team of secure microcontroller, ASIC, and embedded cryptography/security experts (more than 20 years of experience in the security field) with tens of designed and certified secure ICs (EMVCo, EAL5+, FIPS):

- Our team closely works with your team through every step of your product lifecycle to assess and determine the optimal solution for your application, system, or ecosystem.
- Alongside with your team, our team ensures that state-of-the art implementation is done.
- Our team works with your team to analyze and implement solutions to the constraints that such secure design requires for testing and/or production.

Working with StarChip® as your security partner helps you developing a safe and comprehensive solution for a complete success.

ARX SECURE CORE

Arx Secure Core is a High-performance 32-bit RISC core based on Cortus APS3s CPU with embedded secure mechanism. StarChip designers implemented protection against fault injection and side channel attacks on:

- Register bank
- ALU
- Buses

Arx Secure Core can be used as the main CPU of your system or in conjunction with an application processor in case of more demanding applications. Supporting various system interfaces (AMBA...) Arx SecureCore is available in ASIC (synthesizable HDL) and FPGA (netlist) forms, and includes everything required for successful implementation. A development kit (compiler, debugger) is also available.

INVICTE CRYPTO ENGINE

Invicte Crypto Engine is an embedded security module defined as a standalone IP supporting the main industry-standard algorithms:

- PKA (Public Key Accelerator) for RSA and ECC calculations
- AES (Advanced Encryption Standard)
- DES (Data Encryption standard)
- HASH algorithms (MD5, SHA)
- RNG (Random Number Generator)

Invicte Crypto Engine combines StarChip® expertise in both Cryptography and Embedded security and gives the user flexibility to configure the implemented algorithms. It is scalable to be adapted to customer's requirements whether a high-performance throughput or the smallest footprint is requested. Our team will help you to accelerate the Invicte Crypto Engine design and test integration and thus optimize your Time To Market.

...IRON-CLAD SECURITY

EFFICIENT IN EVERY ASPECT ...

... COST EFFECTIVE

TURBOSECURE

In a competitive environment of escalating pricing and margin pressure, cost control also plays a critical role. Reducing production expenses by even one or two percent can mean all the difference in maintaining a competitive organization. Solid security is just one of the many concerns involved in uploading software during production. The StarChip® TurboSecure Uploading System lets manufacturers enjoy significant cost savings in production time and costs for a variety of applications. This streamlined communications system has been designed to accelerate and secure software uploading in mass production environments. Enhancing ISO communication mechanisms enables us to perform 0.5Mbps programming for our products, including transmission and decryption. Our Product Decryption Unit (PDU) enables on-the-fly decryption, without interfering with flash loading.

SECURE LIFECYCLE

Manufacturing costs represent the largest share of chip production expenses. To help control costs, OEM and fabless design companies utilize offshore, low cost foundries, potentially saving millions of dollars. However, to fully realize the benefits of this strategy, offshore foundries must be supported by robust, secure lifecycle management technology that can protect products against IP hacking, counterfeit attempts, and gray market threats. StarChip®'s secure, advanced lifecycle management technology enables our customers to unlock the benefits of low cost, offshore manufacturing, without compromising on IP security.

CERTIFICATION

StarChip® experts can assist you with the main certification standards which are EMVCo, Common Criteria and FIPS. Our objective is to help you to win Time To Market and to avoid iterations by relying on our people knowledge/expertise and by engaging the process as early as possible in the product Lifecycle. This makes the certification process easier and cost effective. Our mission is to assist you in the certification of the product and the creation of the necessary documentation required by the third party labs.