

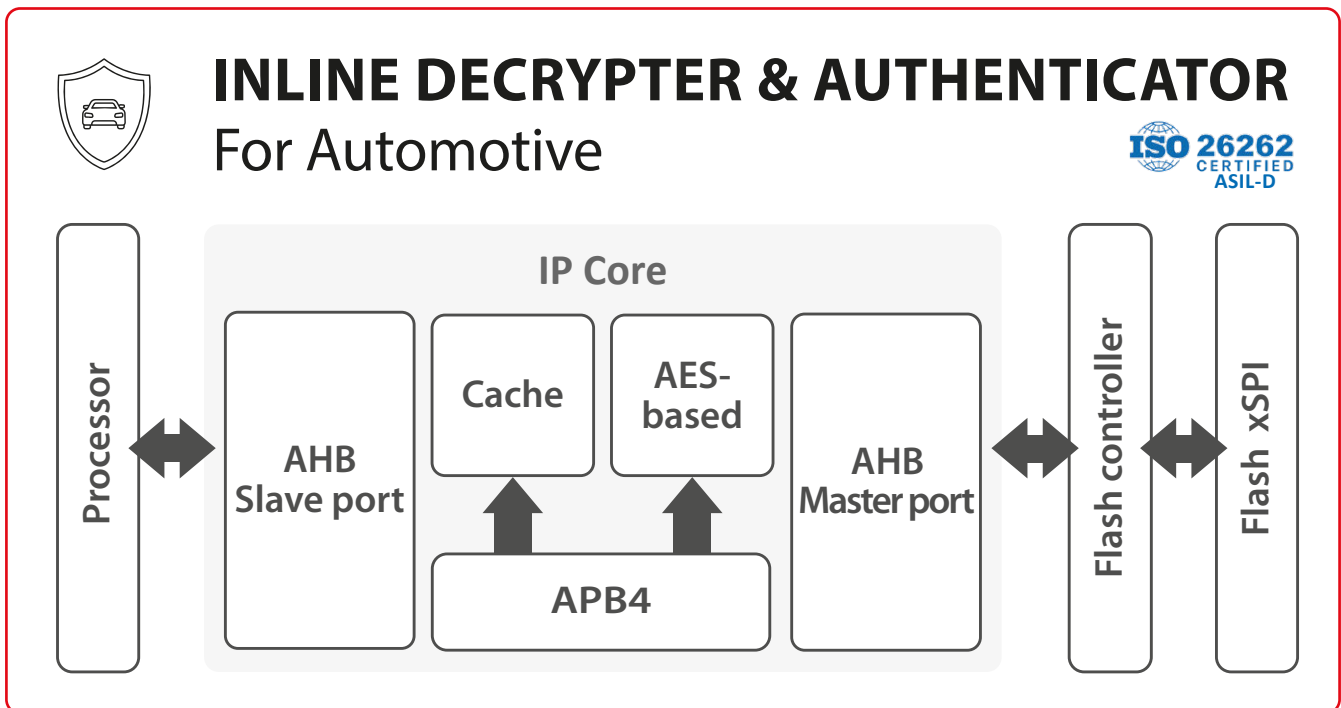
INLINE DECRYPTER & AUTHENTICATOR FOR AUTOMOTIVE



The Inline Decrypter and Authenticator IP core enables on-the-fly execution of encrypted and signed code from Flash. It is used to authenticate and decrypt code located in Flash. In addition it is ISO26262 certified (ASIL-D).

This solution manages multiple regions with software encrypted and signed with different keys. It includes a cache of configurable size and supports AHB interfaces

With this IP core, our customers can take advantage of our expertise in ASIC and FPGA design, cryptography & security applications and the development & integration of re-usable cores & high-level IP solutions. DPA countermeasures option available for applications requiring higher level of security with a very good protection against SPA (Simple Power Analysis) and DPA (Differential Power Analysis).



Features

- ✓ XIP (eXecution In Place) of encrypted and signed code from Flash
- ✓ ISO26262 certified (ASIL-D)
- ✓ AHB Master/Slave interfaces
- ✓ Authenticated decryption or authentication only - defined per region
- ✓ Scalable cache solution
- ✓ SPA/DPA countermeasures (optional)
- ✓ Supports multi-region
- ✓ Scalable amount of regions
- ✓ Secure boot
- ✓ ASIC and FPGA

Applications

- ✓ Automotive
- ✓ General purpose MCU

Implementation aspects

The unique architecture enables a high level of flexibility. The throughput and features required by a specific application can be taken into account in order to select the most optimal configuration for any FPGA or ASIC technology. The single RTL database for all configurations is a guarantee of liability and integration is made very easy due to standard interface (AMBA AHB).

Deliverables

- ✔ Netlist or RTL
- ✔ Scripts for synthesis & STA
- ✔ Self-checking RTL test-bench
- ✔ Technical documentation
- ✔ Safety-related documentation (ISO26262)

We are also offering the inline decrypter and authenticator for other applications (i.e. industrial, defence...). For more detailed information, please contact us.

Our memory protection portfolio:

Memory Protection	XiP from Encrypted Flash		External DDR Protection	
	INLINE DECRYPTER	INLINE DECRYPTER & AUTHENTICATOR	DDR ENCRYPTER	MEMORY & BUS PROTECTION
Securely and transparently write/read data or code from external memory. It leverages our AES Core and the unique architecture enables a high level of flexibility (cache size, performances) and allows it to be used by microcontroller and multi-core architectures	Enables on-the-fly execution of encrypted code from Flash. Often used to protect the source code	Enables on-the-fly execution of encrypted and signed code from Flash. It is used to authenticate and code located in flash	Enables on-the-fly encryption and authentication to the external memory	Enables on-the-fly encryption/decryption and authentication to the external memory
Configurable/scalable for perfect application fit	✔	✔	✔	Configurable
Multiple regions management	—	✔	✔	—
Protection scheme	Decryption only	Authentication & Decryption	Authentication & Encryption or Encryption only	Authentication & Decryption
Performance	Suitable for up to O-SPI DTR @200 MHz	Suitable for up to O-SPI DTR @200 MHz	ASIC: 100 Gbps FPGA: 40 Gbps	ASIC: 15 Gbps FPGA: 3 Gbps
DPA countermeasures	✔	✔	—	✔
ASIC / FPGA	✔	✔	✔	✔
Scalable data bus width	32	32	32, 64, 128, 256, 512 bits	32, 64, 128 bits
Power/area	Scalable	Scalable	Scalable	Scalable
Interface support	AHB	AHB	AXI	AHB, AXI
SECURE-ic THE SECURITY SCIENCE COMPANY	PRODUCT CODE SCZ_IPX_BA432a	PRODUCT CODE SCZ_IPX_BA432d	PRODUCT CODE SCZ_IPX_BA432c	PRODUCT CODE SCZ_IPX_BA432b

V1.1

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