SILEX INSIGHT

eSecure module for SoC security

BA470

The eSecure IP is a single subsystem for SoC/ASIC/FPGA to address key security challenges, playing the role of root-of-trust. The module is highly flexible and fits all applications of the heterogeneous Internet-of-Things ecosystem, from the ultra-low power sensor to the connected car.

Single module for multiple security challenges

Hardware Root of Trust

One of the key elements of a secure device is to execute authenticated and trusted software in order to prevent malicious code execution. The eSecure IP provides a strong authentication of the software/firmware at boot-time (secure boot) and during run-time. It will also optionally decrypt the code before execution by the host processor.

Device unique identity

In order to protect applications and products against counterfeiting and cloning, it is important to be able to uniquely identify each manufactured part. This identification also enables device authentication and per device right management.

Secure storage of secret information

A secure application always requires some data to be kept secret. The eSecure IP can store secret keys and other information inside a secure or non-secure storage area. For non-secure area such as external flash memories, the eSecure IP will guarantee the confidentiality and authenticity of the data with strong cryptographic algorithms.

Secure communication

In today's connected world, most applications involve secure communication protocols. The eSecure cryptographic engine supports all the latest algorithms for **TLS/DTLS 1.3, Thread Networking, Apple HomeKit, Bluetooth, Zigbee** and more.

Feature Hightlights

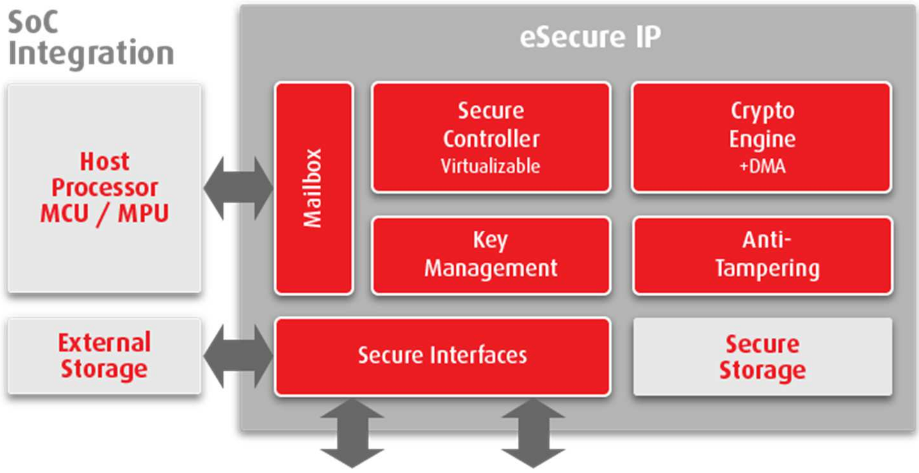
- HW RoT, Secure Boot
- Cryptography algorithms off-loading
- Side Channel Attack protection
- Secure Debugging
- Key Management
- Low power and high performance

Applications

- Smart Cities
- Connected home
- Automotive (C2X)
- Industrial
- Healthcare
- Wearable
- …

Integration of the eSecure IP into a full System-on-Chip

The eSecure IP is a complete standalone module that enables security applications by shielding the secret information from the non-secure application running on the main processor. The firewall prevents any unauthorized access to the secret data. The secure controller embedded in the eSecure module keeps full control of the execution of the security functions. In some designs, the secure controller can be optionally virtualized in the host processor.



Efficient secure hardware solution for any application

The eSecure IP is a very efficient solution to enable any secure application on chip. The hardware module shielded from the main processor brings a high level of security. Also the hardware offloading of the cryptographic operations from the main processor to the eSecure module guarantees a low power operation. The eSecure module is tuned to the target application in terms of feature and performance.

Anti-tampering management

Most secure chips involve one or multiple tamper detection mechanisms. The advanced anti-tampering management unit of the eSecure IP enables fine control of the tamper detection source, and actions to be taken when an event occurs, such as instantaneous zeroisation of the secret data. The configurability of the unit makes it suitable for basic up to advanced security requirements.

Scalable cryptographic engine

The scalable cryptographic engine supports symmetric encryption (AES, DES, …), asymmetric operations (ECDSA, ECDH, RSA, …), hashing (SHA-1, SHA-256, …) and random number generation. The cryptographic engine can be configured to reach the performance level required by your application, enabling efficient offloading of the main CPU.

For more information, please contact us.

Silex Insight
Rue du Bosquet, 7
1348 Louvain-la-Neuve
Belgium

Website	www.silexinsight.com
Email	sales@silexinsight.com
Phone	+32 (0) 10 454 904