Securing the connected world

Flexible and scalable embedded security IP

Pieter Willems

pieter.willems@silexinsight.com

V2.0 – 2019

Overview

- Silex Insight Introduction
- Embedded security markets and applications
- Security requirements
- Scalability and flexibility
- Configurable and scalable secure enclave: eSecure

This is Silex Insight!

What we do: ***IP provider for security in embedded systems***

- Headquarters in Brussels, Belgium
- Global presence
- Worldwide customer base
- Founded in 1991 – 28 years experience
- Silex Insight = Silicon experts with know-how
- 45 employees

A history of growth and innovation

1991 — Founded as ASIC design house in Louvain-la-Neuve, Belgium

1995 — Becomes part of the Barco group

1999 — 1st SoC development for payment terminal

2003 — Introduction of JPEG2000 IP cores for FPGAs

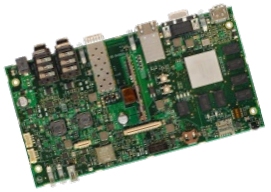
2011 — Introduction of Public Key and AES cryptographic IP cores

2015 — Technology & Engineering Emmy Award for J2K Interop

2016 — Introduction of VIPER (HDMI over IP OEM board) and eSecure: (Embedded Security IP)

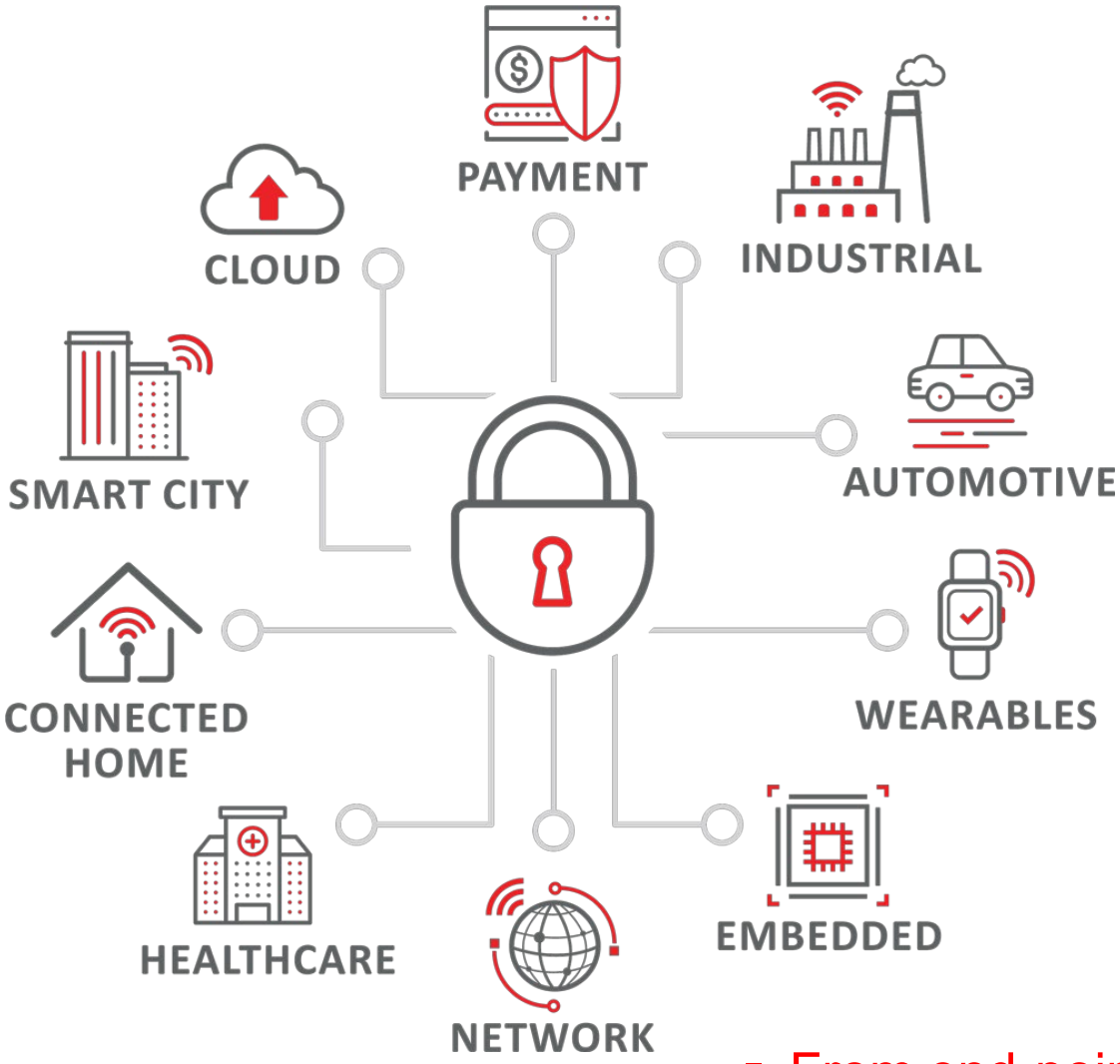
2018 — Barco Silex becomes Silex Insight (Private Equity funded MBO)

2019 — Global presence (US office)



SILEX INSIGHT

Security Markets/Applications



- From end-point, edge device to data center

SILEX INSIGHT

Security requirements

Features/solutions

SECURED SYSTEM-ON-CHIPS (SOC)

DEVICE UNIQUE IDENTITY

SECURE STORAGE OF SECRET INFORMATION

SECURE DEBUGGING

SIDE-CHANNEL ATTACK PROTECTION

SECURE COMMUNICATION

Security requirments

Algorithms/modes and protocols

- Asymmetric algorithms
  - RSA/DH/DSA/CRT/ECC/ECDSA/ECDH
    - ECC Curves: NIST, Brainpool, Koblitz, Montgomery, Edwards and others…
  - Apple HomeKit/TLS1.3: Curve25519, EdDSA, SRP
  - Thread Protocol: J-PAKE
  - Rabin-Miller (primality check) and Key Generation
  - SM2 (OSCCA), EC-KCDSA, ECIES, ECMQV
- Random Number Generators
  - TRNG (NIST 800-90B and AIS-31)
  - DRBG (NIST 800-90A)
- Symmetric algorithms
  - AES supporting all modes (GCM, CCM, CFB, CBC…)
  - Ultra High performance AES-GCM/CTR/XTS
  - 3GPP algorithms (Snow3G, Kasumi, ZUC)
  - Chacha20_poly1305 – TLS 1.3/Apple HomeKit
  - SHA1/2/3, SM3 (OSCCA) & 3-DES core
  - SM4 (OSCCA)
- Secure communication protocols
  - TLS/SSL
  - IPsec
  - MACsec

Security requirments

Application and market specifications

- Performance
  - Asymmetric crypto
    - High perf: V2X, fast boot apps, crypto currency, TLS connection engine
    - Low perf: IoT end-points
  - Symmetric crypto (incl IP/MACsec)
    - High perf: DC/cloud, networking, automotive
    - Low perf: IoT end-points
- Power
  - IoT end points: Low power requirements
  - Others: flexible power requirements
- Resources
  - Optimal resource/perf ratio: IoT end-points
  - Flexible: DC/cloud, networking
- Features
  - IoT: wide variety of features, protocols/radio (crypto) to be supported
  - DC/cloud: limited modes/protocols but at high speed and wide variety of features required

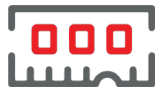
SILEX INSIGHT

Combinable products

Configure it, the way - YOU - want it!

Security enclave

eSecure ROT provides full system security



Memory protection

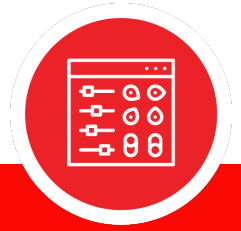
Secure your flash and DDR

Networking solutions

Accelerate your complete TLS, MACsec and IPsec traffic

Crypto accelerators & processors

Accelerate your crypto operations



CONFIGURABLE
Include features as needed

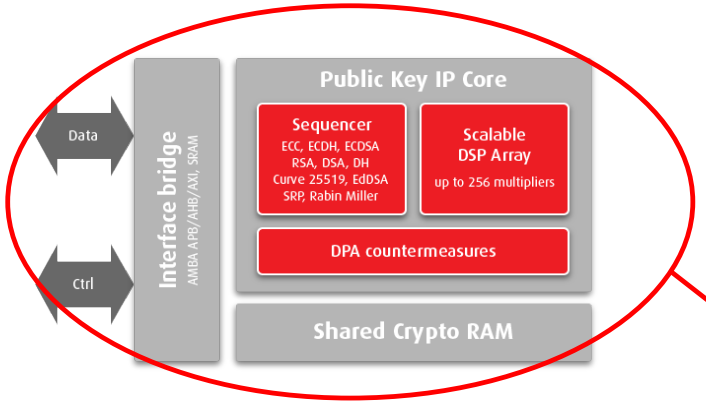
SCALABLE
Define performance and footprint depending on your requirement

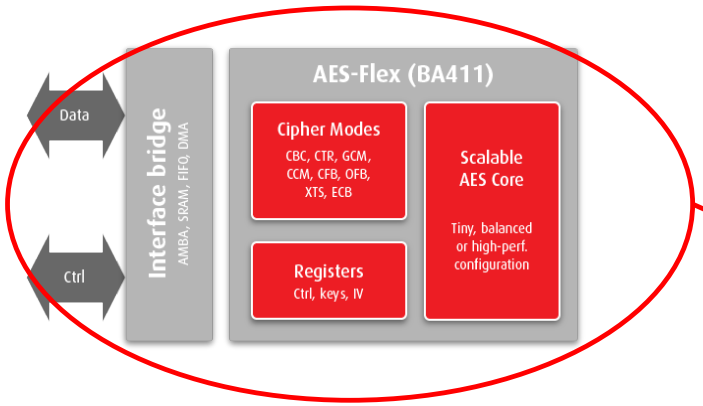
CUSTOMIZABLE
Adapt to your specific needs

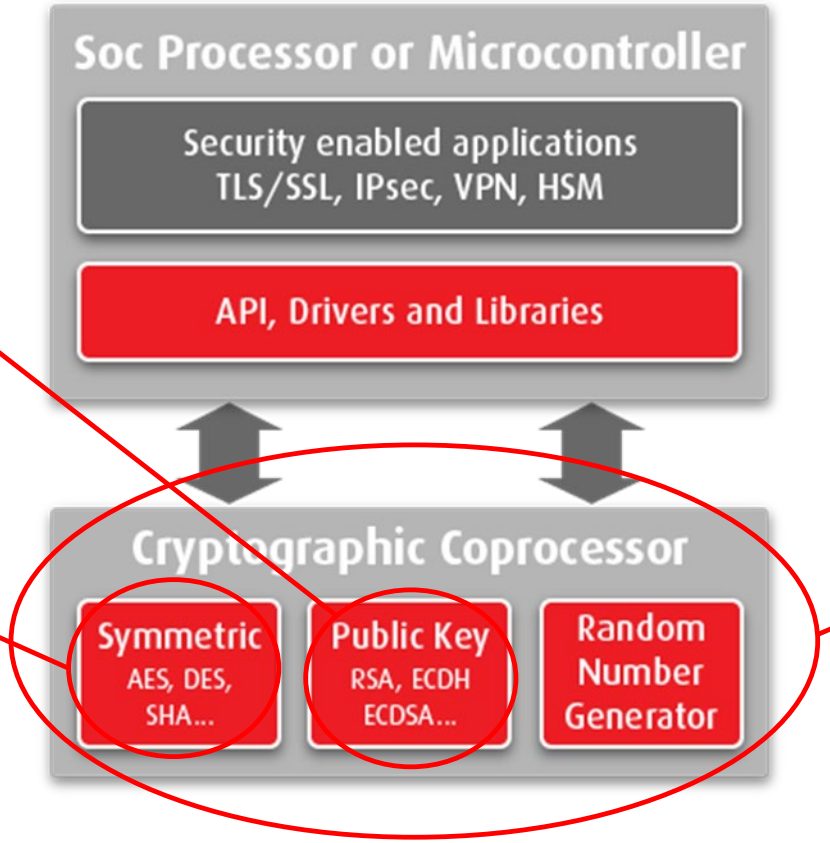
SILEX INSIGHT

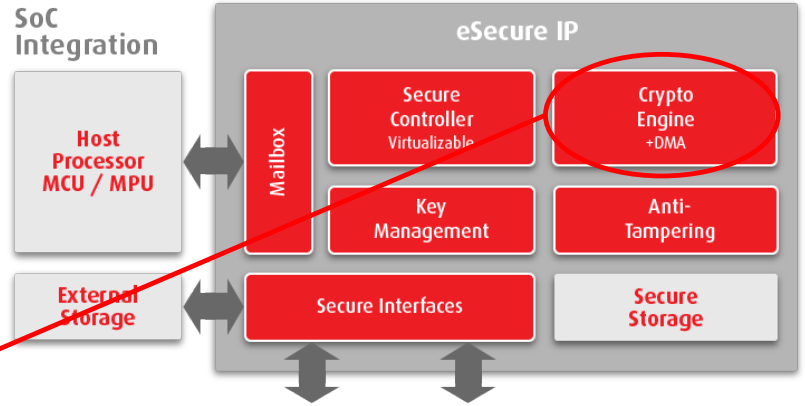
Scalability

From block to solution









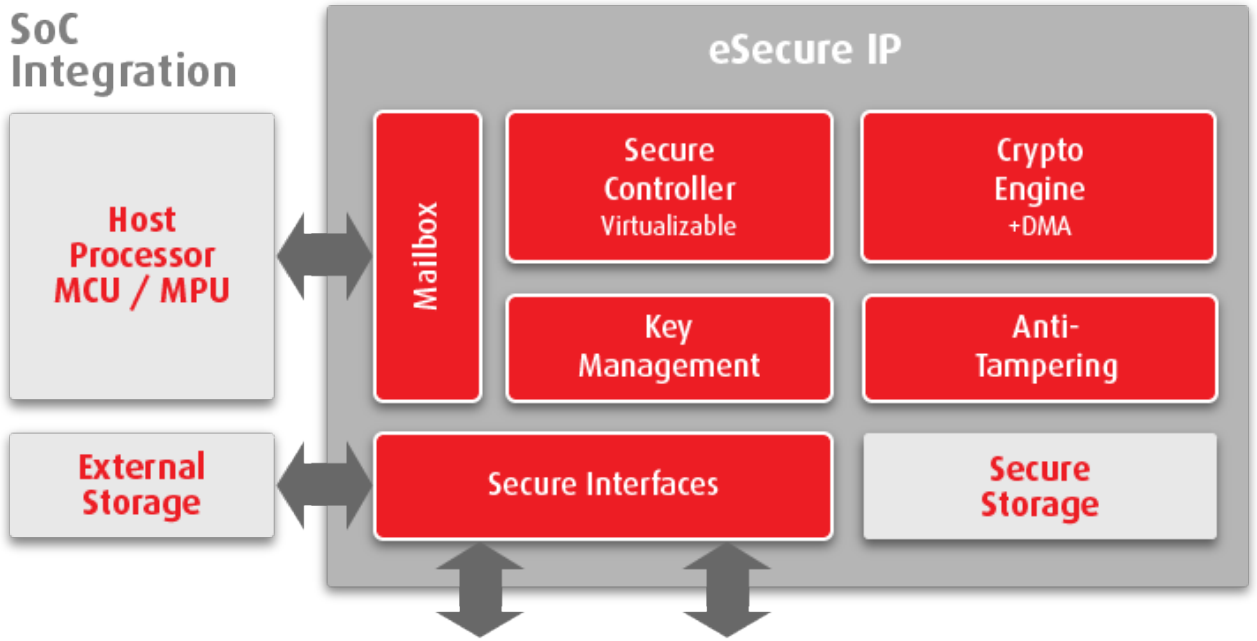
Stand-alone, scalable, flexible and configurable cores for perfect application fit

Combined into scalable and configurable crypto accelerator

Added to scalable and flexible secure enclave to target any connected device SoC

eSecure: BA470

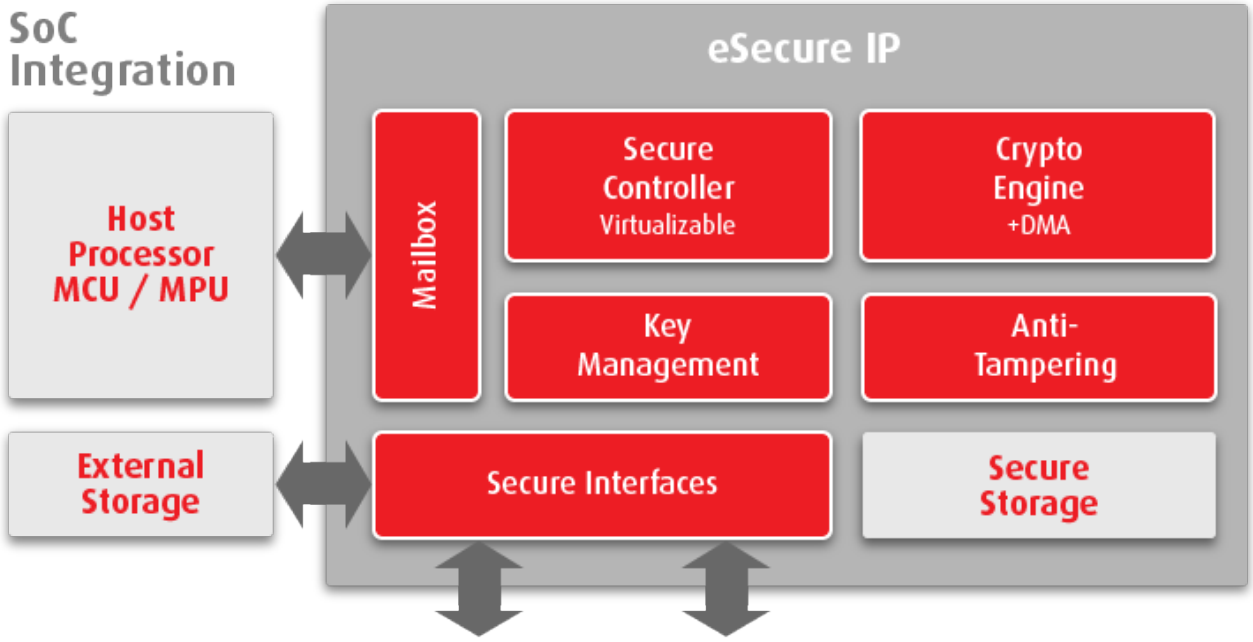
- Security Enclave - HW Root-of-trust
- Scalable and flexible solution to serve many IoT markets/devices
- Offer secure services to the Host (via mailbox)
- EVITA compliance + AutoSAR API



eSecure: BA470

Configurable features

- eSecure (HW Root Of Trust, Security Enclave)
  - Secure Boot
  - Secure Debugging
  - Secure Key Storage
  - Device Authentication
  - Anti-tampering – Side Channel Attack protection
  - PUF available
  - Low power features (retention, power down)
  - Several processors integrated
    - RISC-V Controller (from various partners)
    - ARM
    - MIPS
  - Wide range of cryptographic algorithms
  - Silicon proven

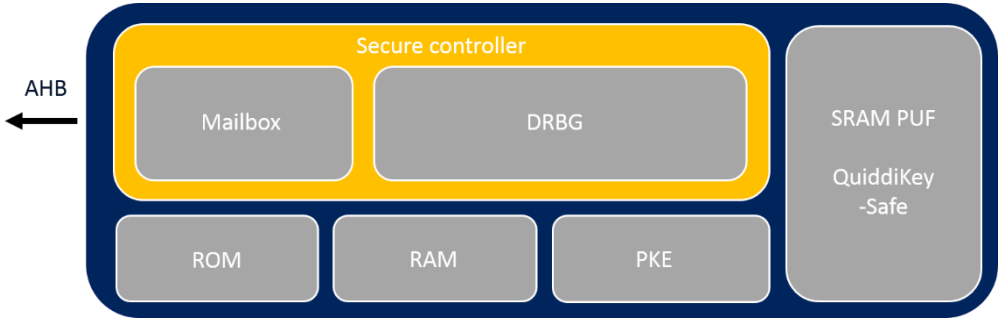


- Applications: Automotive, Industrial, DC/Cloud computing, IoT end Node device, Wireless communications

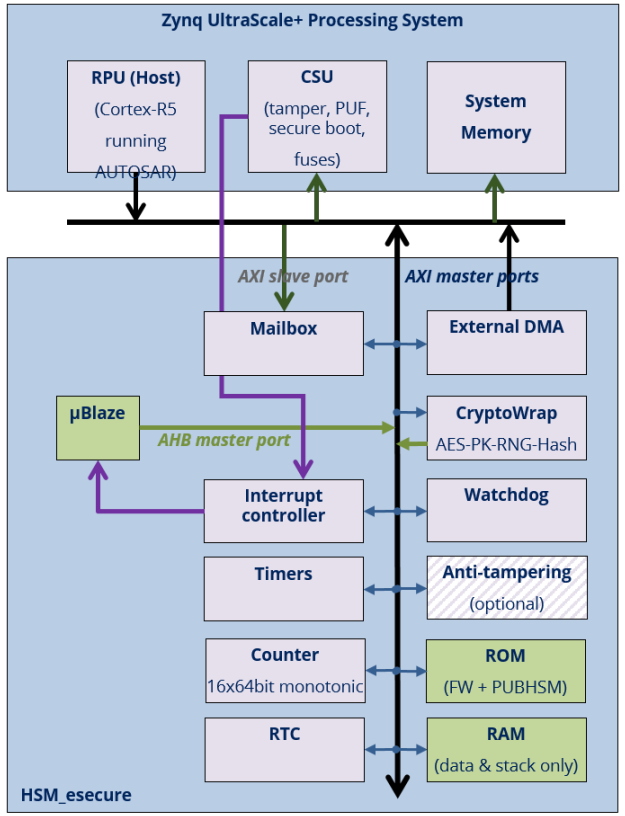
Flexibility example

KeySecure + eSecure for FPGA

- KeySecure (with intrinsic ID)
  - Securely generates, stores and manages any type of key
  - No access to keys by the host



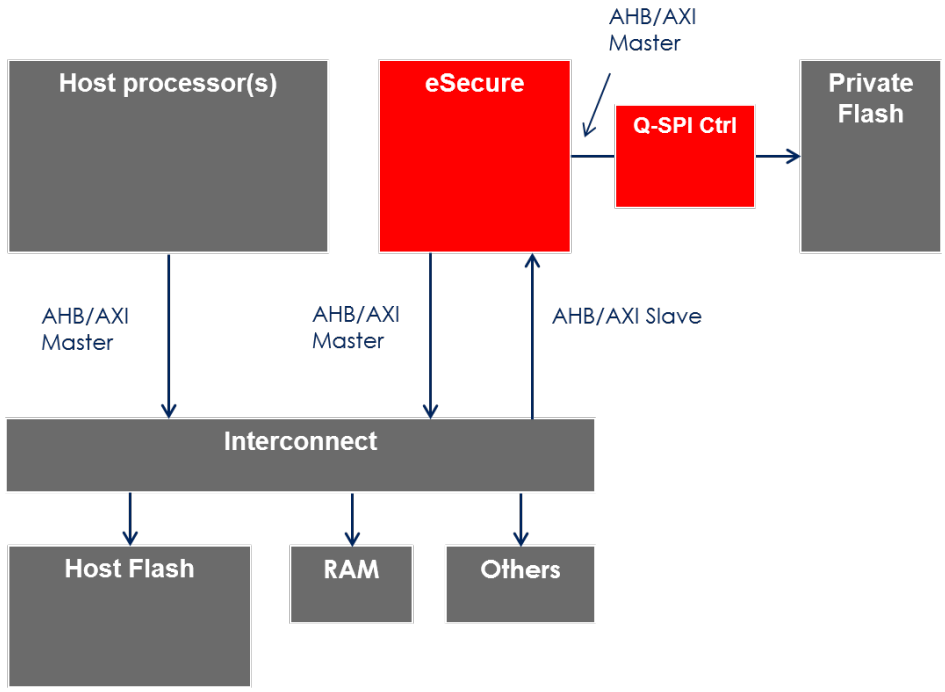
- eSecure-HSM
  - FPGA HSM for industrial and automotive applications
  - EVITA compliant



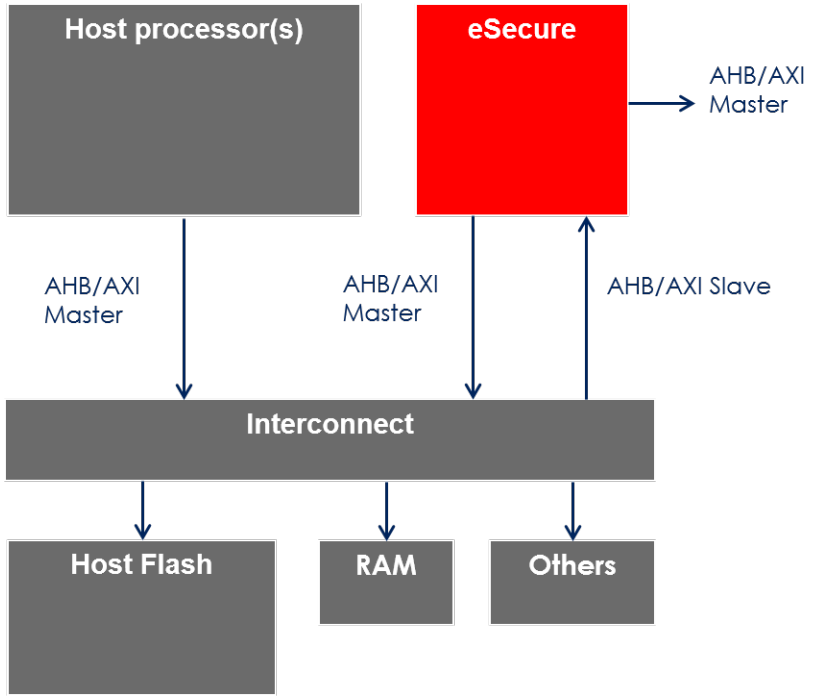
SILEX INSIGHT

Integration Flexibility

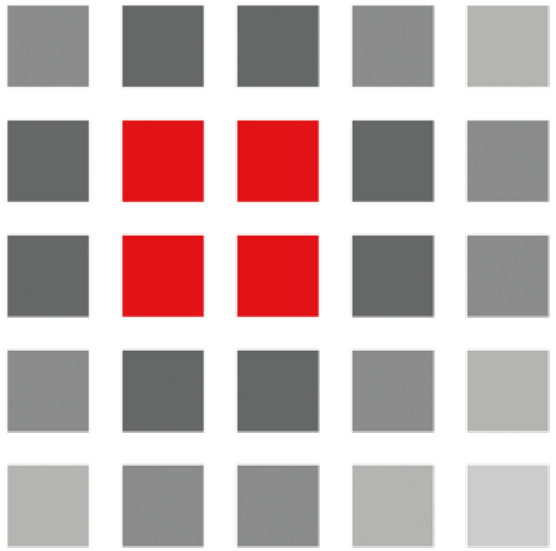
Private/host flash



- Private Flash
  - Embedded
  - External



- Host Flash
  - Embedded
  - External



SILEX INSIGHT

EMBEDDED IN YOUR FUTURE

www.silexinsight.com

sales@silexinsight.com

support@silexinsight.com