



HARDWARE SECURITY MODULE

For automotive applications

Presented by Pieter Willems

Pieter.willems@silexinsight.com

December

What we do: ***IP provider for security and video 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





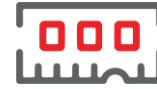
Choose single or a complete module

We build for your specific needs



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

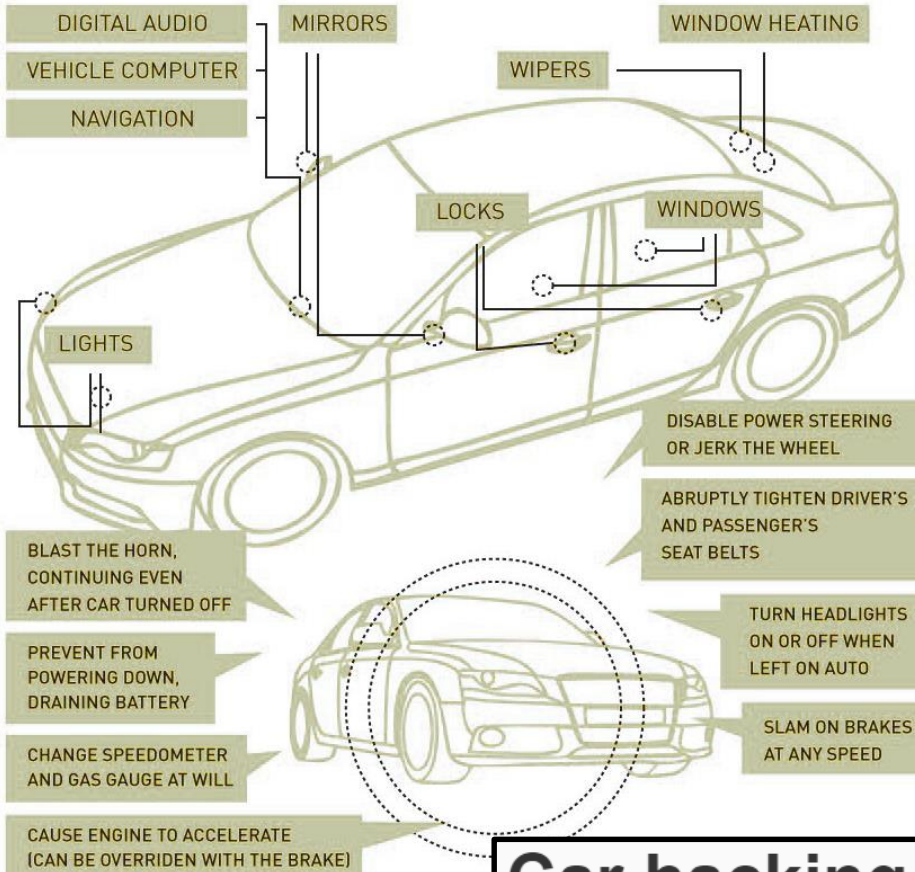
CUSTOMIZABLE

Adapt to your specific needs

- Ever-increasing number of connected cars
- Many applications
 - Infotainment
 - ADAS
 - V2X gateway
 - Power systems
 - Comfort/safety systems
- Gartner identifies “trusted cars/hardware” as part of the Top 3 autonomous driving technologies



Connected Car Security Threats



KIM ZETTER SECURITY 07.10.12 3:29 PM

GONE IN 3 MINUTES: KEYLESS BMWs A BOON TO HACKER THIEVES

New vulnerability lets attackers hijack Chrysler vehicles remotely

Hackers were able to remotely control a moving Tesla Model S

Car hacking remains a very real threat as autos become ever more loaded with tech

- Securing a connected car and its sub-modules is all about trust
 - Trust Firmware running on your module?
 - Identity of modules and other connected cars?
 - Secure communication channel?
 - Privacy
 - Authenticity
 - Integrity



- What is the lifetime of your car/module?
 - Consumer electronics – few years
 - Industrial, automotive, infrastructure – up to 10s of years
- How to handle ownership changes
- Software is susceptible to bugs and must be updated over the product lifecycle
 - Firmware updates in the field required
 - How will these updates be performed securely?



SILEX
INSIGHT

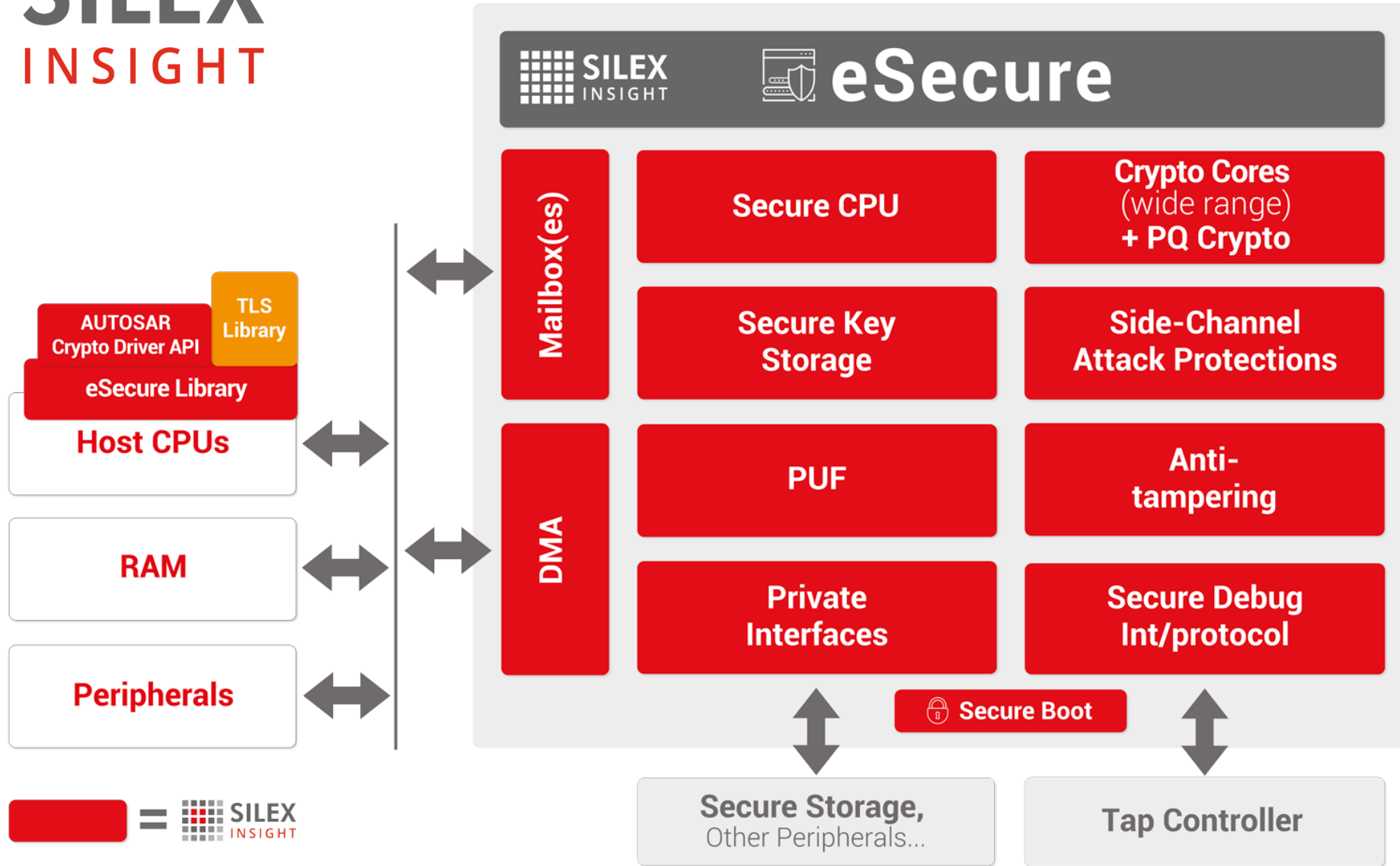
Solution: HSM



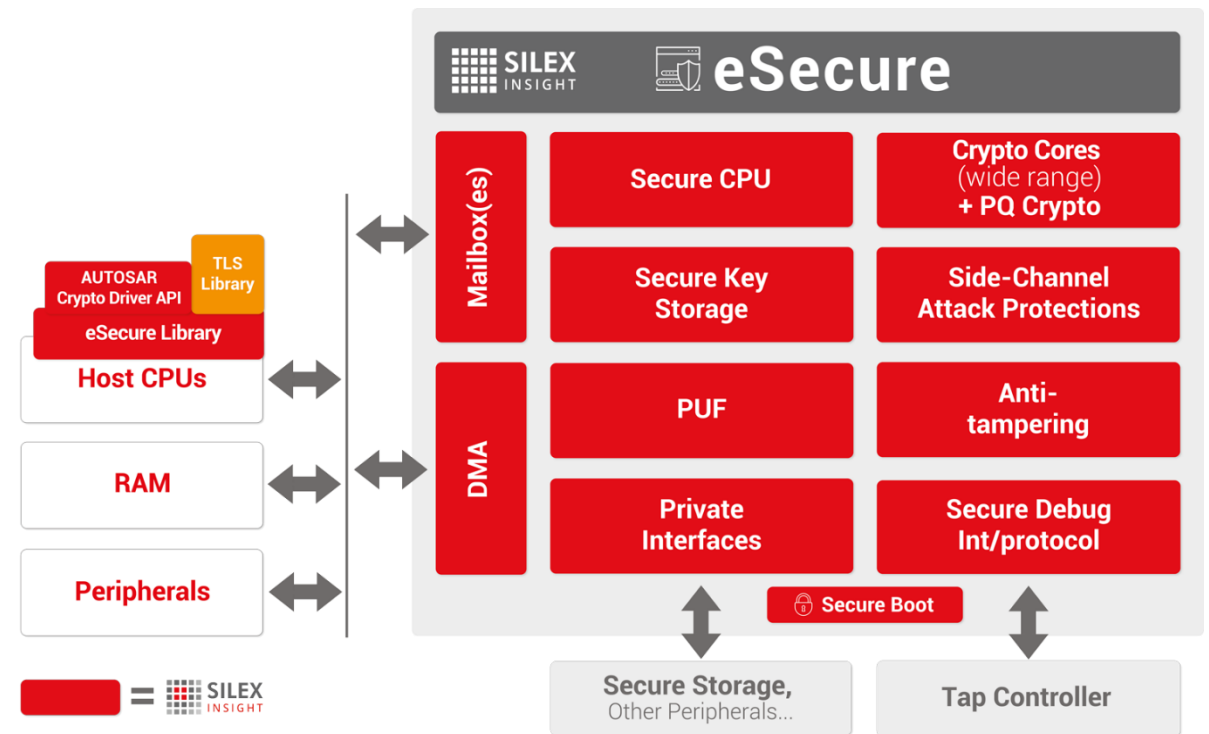
A **hardware security module (HSM)** safeguards and manages digital keys for strong authentication and provides crypto processing.



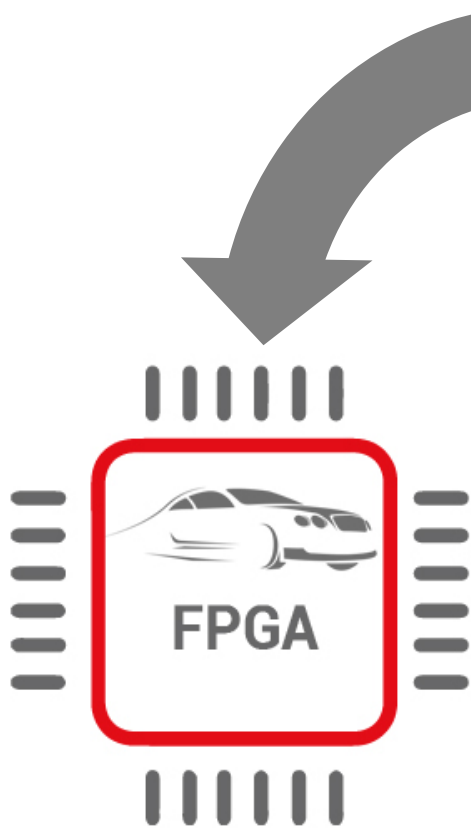
SILEX INSIGHT



- Security Enclave/Root-of-trust
- Firewall between application and secure module
- Flexible and scalable solution using any processor



- eSecure contains a flexible crypto off-loading block
- Wide range of cryptographic algorithms available
 - Asymmetric: RSA/ECC/ECDSA/Curve25519/EdDSA/SRP/J-PAKE ..
 - Symmetric: AES/SHA/ChaCha20-Poly1305/ARIA...
 - TRNG + DRBG (NIST 800-90A/B/C)
- Algorithms specific to the Chinese market also available
 - Asymmetric: SM2/SM9
 - Symmetric: SM3/SM4
- Post-quantum cryptography (PQC) algorithms also available

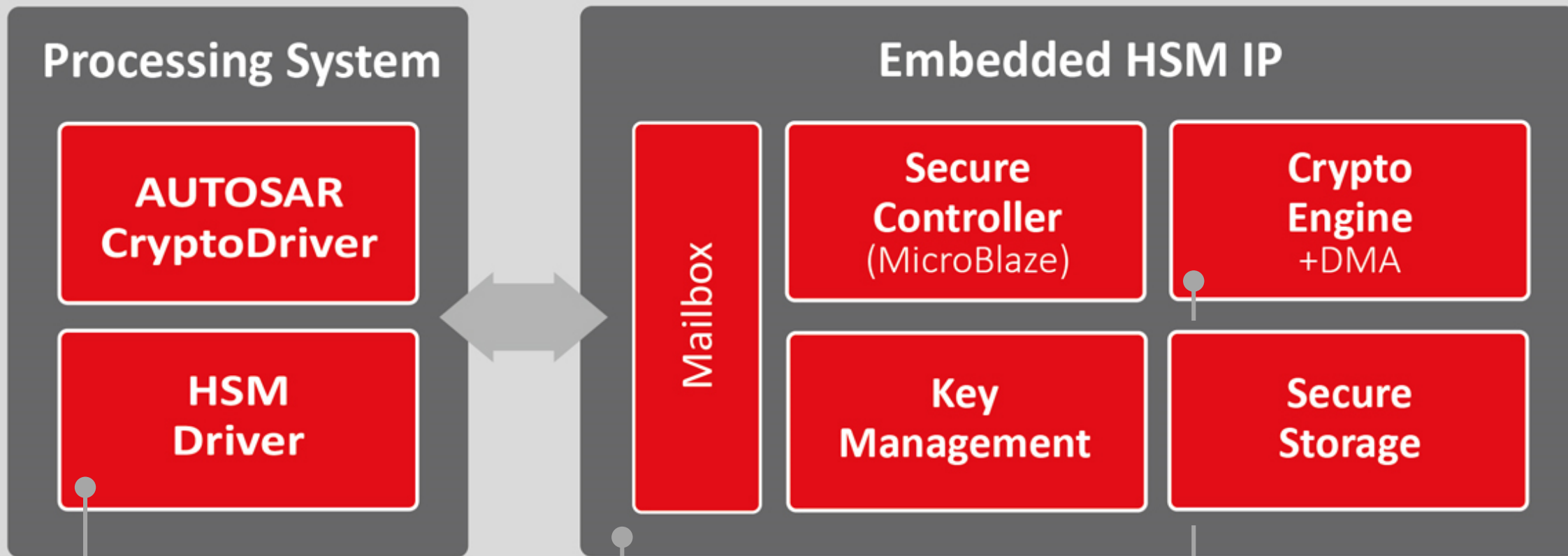


A **hardware security module (HSM)** safeguards and manages digital keys for strong authentication and provides crypto processing.



HSM FOR AUTOMOTIVE

For Xilinx Zynq UltraScale+ MPSoC

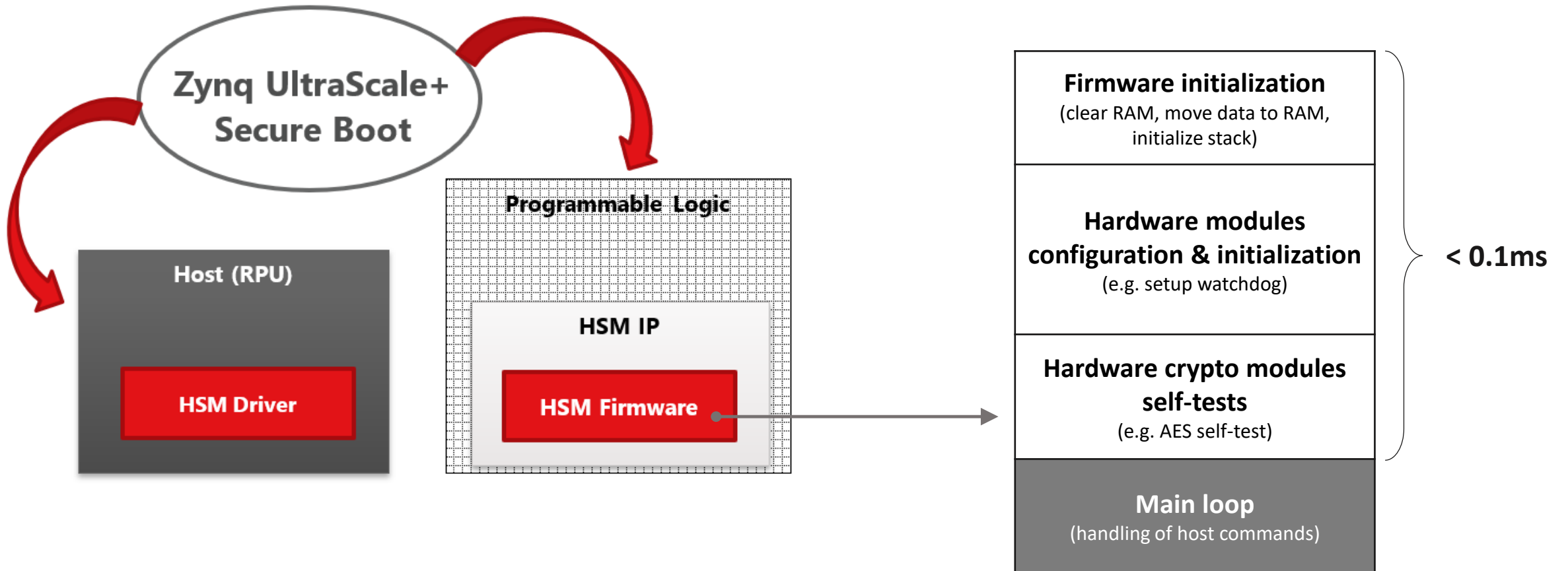


● **Software stack available**

● **Scalable** (Tradeoff features, area, performance)

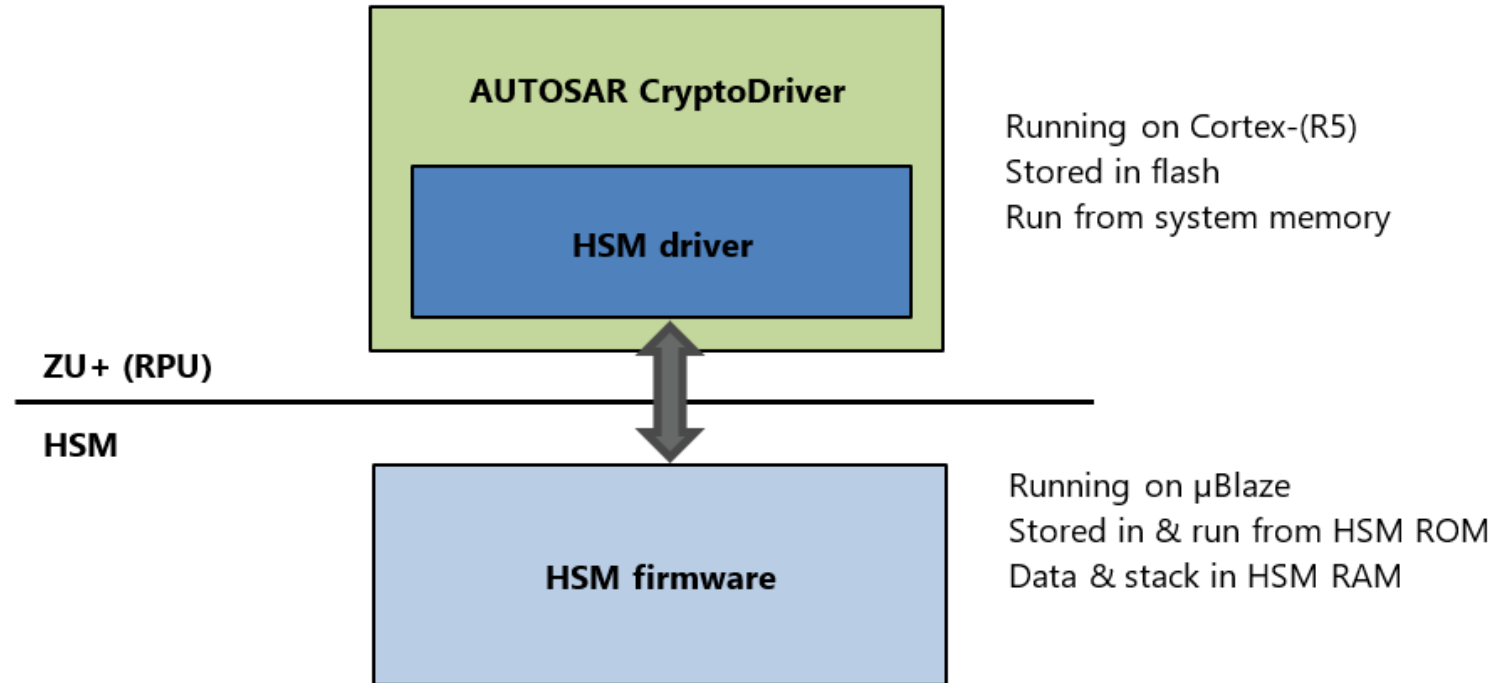
● **Configurable** (All common algorithms supported)

Boot process



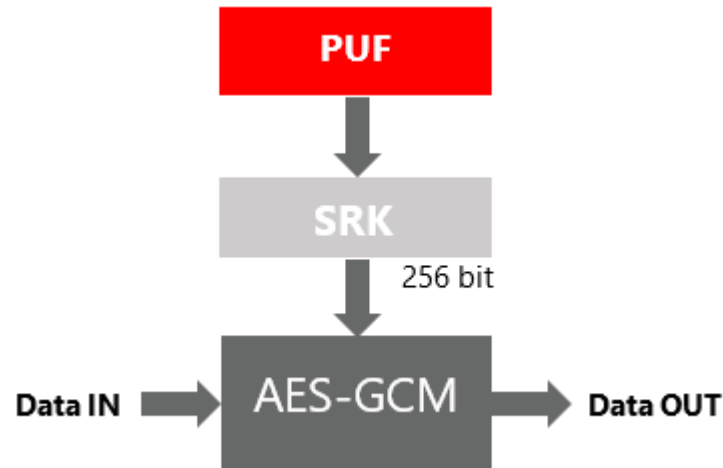
- HSM Driver
 - For non-AUTOSAR applications
 - Bare-metal support only

- AUTOSAR CryptoDriver
 - AUTOSAR R4.3.1 compliant
 - Wrapper around HSM driver



Option 1 – Based on key from PUF

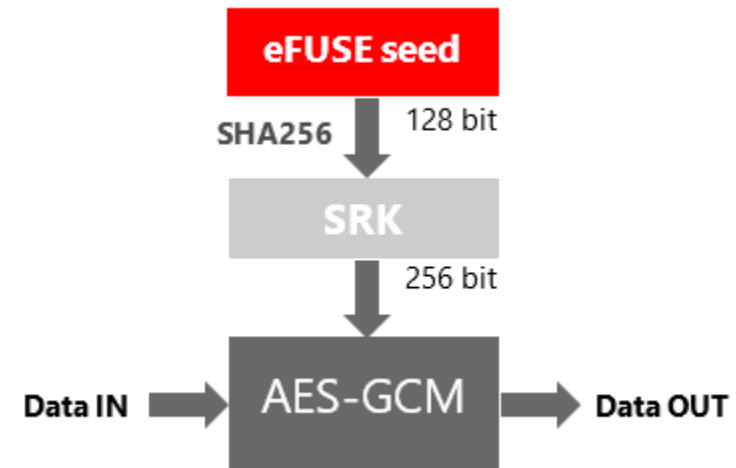
- Storage Root Key (SRK) generated by the PUF



- Unique per device
- Requires PUF (ordering code)
- Requires Hardware Root of Trust boot (no RMA)
- Can use only AES-GCM in CSU

Option 2 – Based on key from eFUSEs

- Storage Root Key (SRK) generated from eFUSE seed



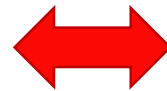
- Could be unique per device
- Requires seed initialization
- Requires 128 user eFUSEs (limited resource)
- Can use AES-GCM in the CSU or PL

HSM

- Configuration of CSU tamper responses
- CSU tamper status reading and clearing
- CSU tamper trigger

CSU tamper sources

- CSU register
- MIO pin
- JTAG toggle
- PL SEU
- Temperature alarm
- Voltage alarm



CSU tamper responses

- Interrupt (custom response by host)
- System reset
- Secure lockdown
- BBRAM erase

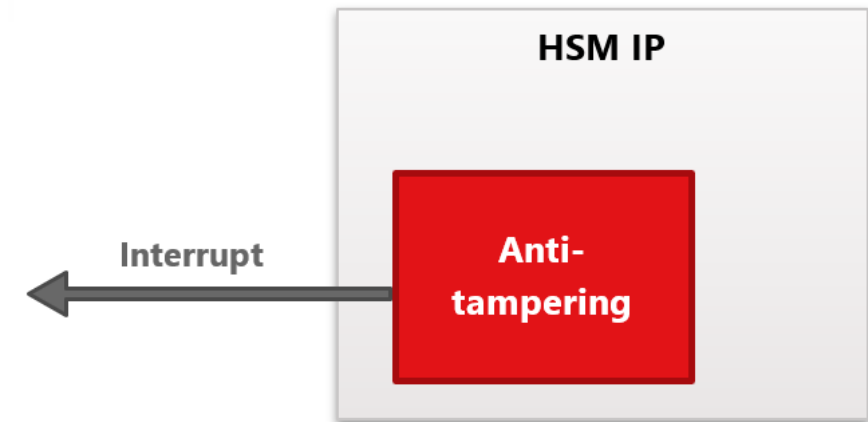
Anti-tampering

HSM contains its own anti-tampering module

Since the HSM is security critical, all detected errors are considered tampers.

HSM tamper sources

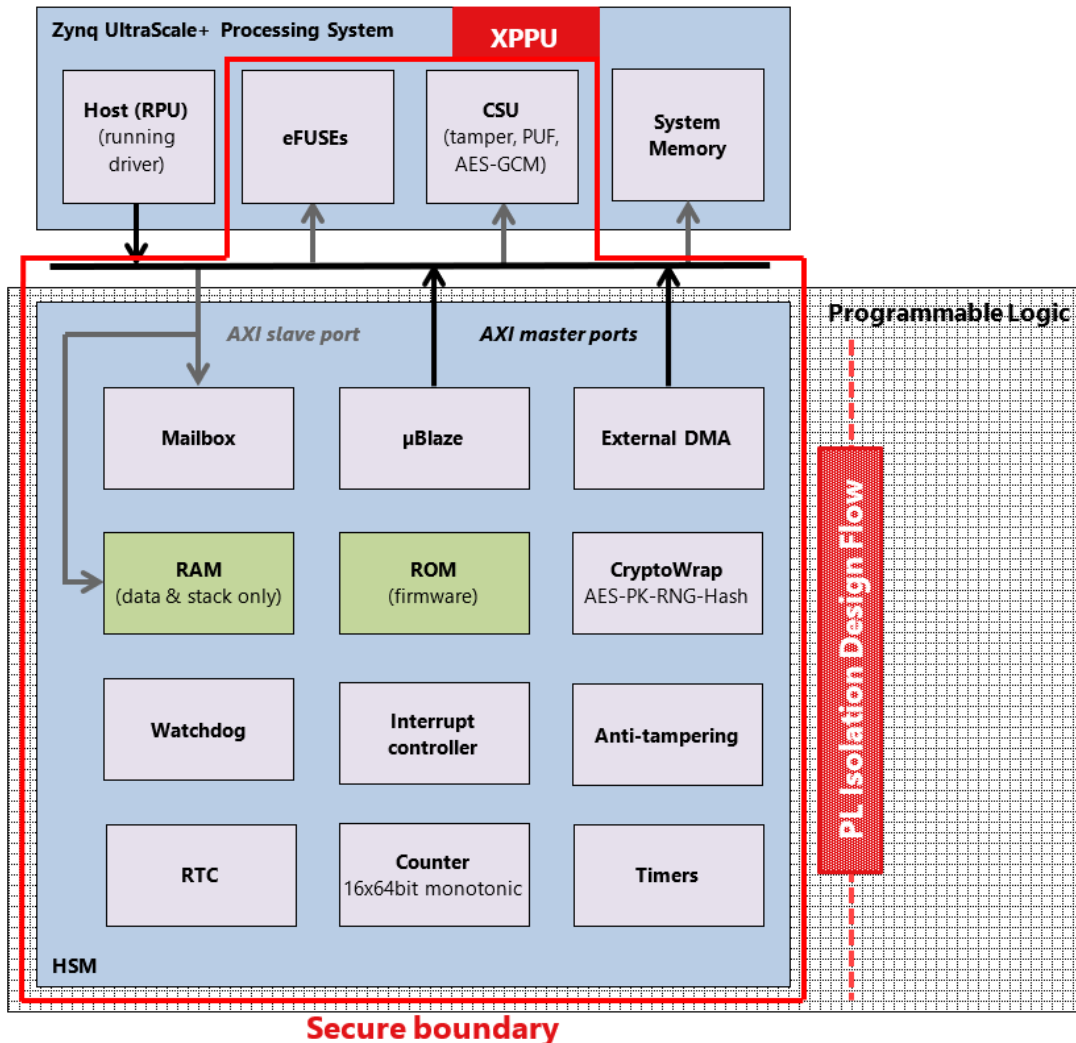
- Watchdog timeout
- RAM CRC error
- RAM unauthorized access
- Hardfault
- Software assertion
- Command authorization error
- Periodic integrity check error
- Self-test error
- TRNG health test error



HSM tamper responses

- Level 1: interrupt
- Level 4: above and wait for reset (halt CPU)
- Level 5: above and trigger CSU tamper response

Ensuring the secure boundary of the HSM



- Xilinx Peripheral Protection Unit to provide HSM exclusive access to
 - CSU
 - CSU DMA
 - eFUSEs

Boot mode ← Configure and lock XPPU → **HSM mode**

- CSU functions directly available
- eFUSEs directly available
- XPPU not configured
- CSU functions partly available through HSM only
- eFUSEs available through HSM only
- XPPU configured and locked
- Xilinx Isolation Design Flow ([XAPP1335](#)) in PL can provide extra robustness

Frequently Asked Questions

■ What is the resource usage?

Device	LUT	FF	DSP	BRAM
ZU11EG	6%	3%	0,2%	6%
ZU7EV	8%	4%	0,4%	11%
ZU5EV	16%	8%	0,6%	25%
ZU4EV	22%	11%	1,0%	28%
ZU3EG	27%	14%	1,9%	17%
ZU2EG	41%	20%	2,9%	24%

*All ZU+ devices are supported

■ Can I remove or add functionality to the HSM IP?

- Yes. Generic statements allow removing or adding functionality, depending on the required features and footprint. A robust library of cryptographic IPs is available for integration.

■ What are the deliverables?

- Netlist or RTL
- Reference design
- Firmware binary
- Driver source code
- Self-checking testbench
- Documentation

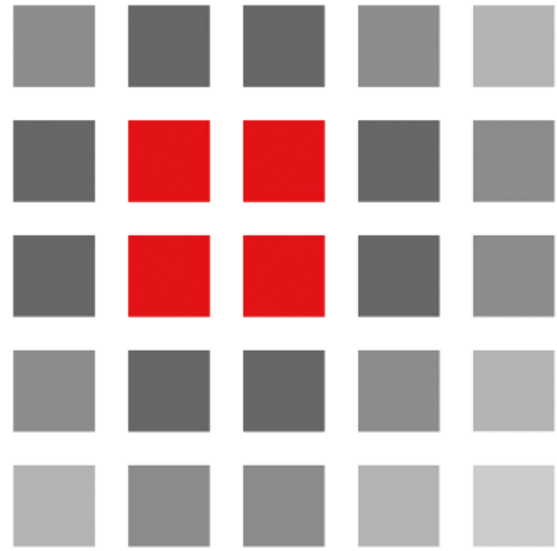
■ What is the business model?

- Silex has a conventional IP licensing model, with license fee, royalties and annual support. NRE and design services are also available through Silex.

- Silex Insight HSM IP addresses security needs across multiple markets
 - Cryptographic offloading
 - Secure key management
 - Secure key storage
 - Flexible and scalable

- Smart integration to Zynq UltraScale+ MPSoC enables adding security to a complex design

- Further investments on features and functional safety planned



SILEX

INSIGHT

EMBEDDED IN YOUR FUTURE

www.silexinsight.com

sales@silexinsight.com

support@silexinsight.com