SILEX INSIGHT

SECURITY ENCLAVE

Based on RISC-V

Presented by Christopher Beaver

Christopher.Beaver@silexinsight.com

14th November 2019

Introduction

The growing Internet of Things

- Ever-increasing number of connected devices
- Many applications
  - Automotive / Transport
  - Healthcare
  - Smart Cities
  - Home automation
  - Industrial
- Gartner identifies “trusted hardware” as part of the Top 10 Internet of Things technologies

SILEX INSIGHT

The risks of IoT

Effect on businesses

Connected medical devices: The Internet of things-that-could-kill-you

By Andrea Peterson August 3, 2015

(BigStock)

Cybersecurity researchers have warned that hackers can hijack cars and even rifles. Now, federal regulators are warning that a pump used to deliver medicine to patients is at risk of being breached.

- Increasing number of devices and applications means more attack surfaces
- A business' reputation can be damaged through bad publicity
- Intellectual property may be copied, leaked or compromised
  - Loss of competitive advantage

SILEX INSIGHT

Securing your device

Basics

- The required level of security depends on many factors
  - Physical access?
  - Public network – possible to intercept communication?
  - Can a single device compromise the entire network?
  - Safety/financial impacts?
  - Who is your attacker?

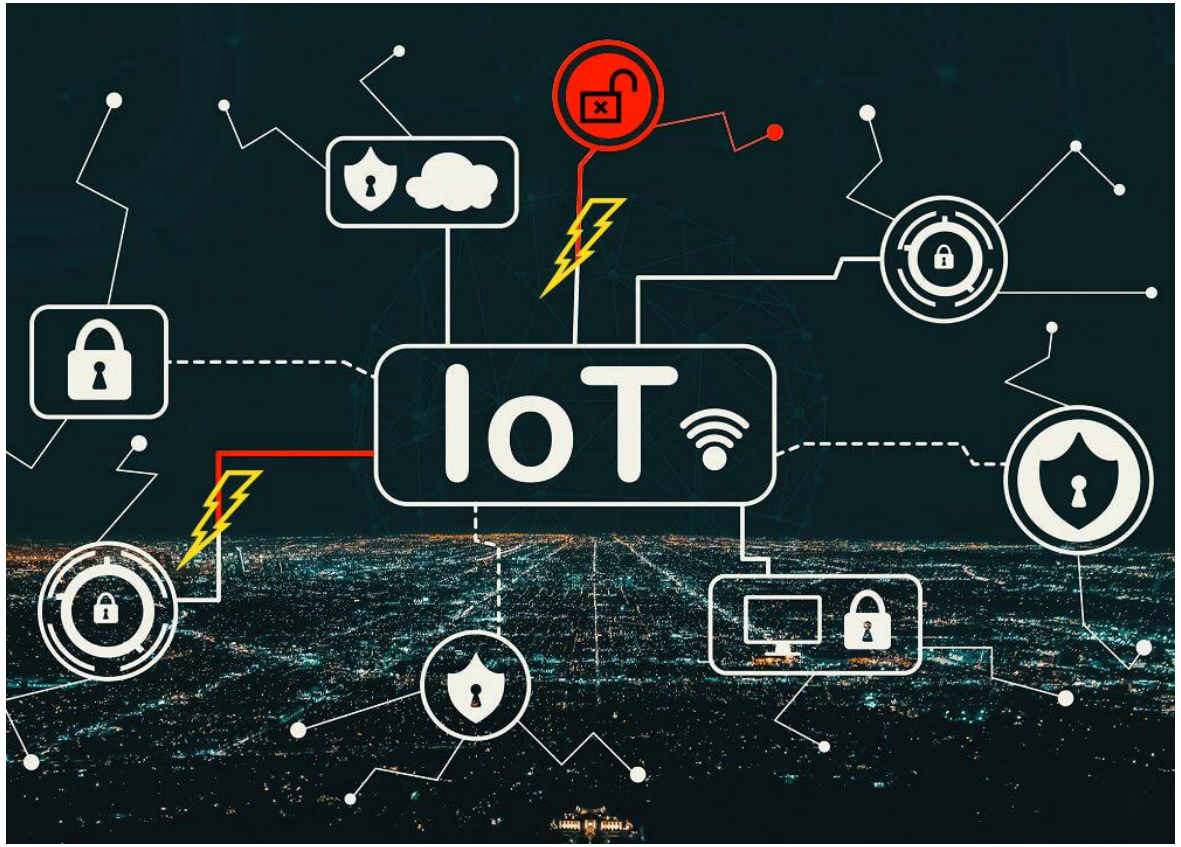
- Risk assessment - threat model

- All above must be considered during the design phase of the product

Securing your device

Trust

- Securing IoT devices is all about trust
  - Firmware running on your device?
  - Identity of other connected devices?
  - Secure communication channel?
    - Privacy
    - Authenticity
    - Integrity



SILEX INSIGHT

Securing your device

Product lifetime

- What is the lifetime of your product?
- Generally speaking
  - Consumer electronics – few years
  - Industrial, automotive, infrastructure – up to 10s of years
- Software has bugs and attacks evolve over the product lifecycle
  - Firmware updates in the field required
- Secure debugging required for some applications

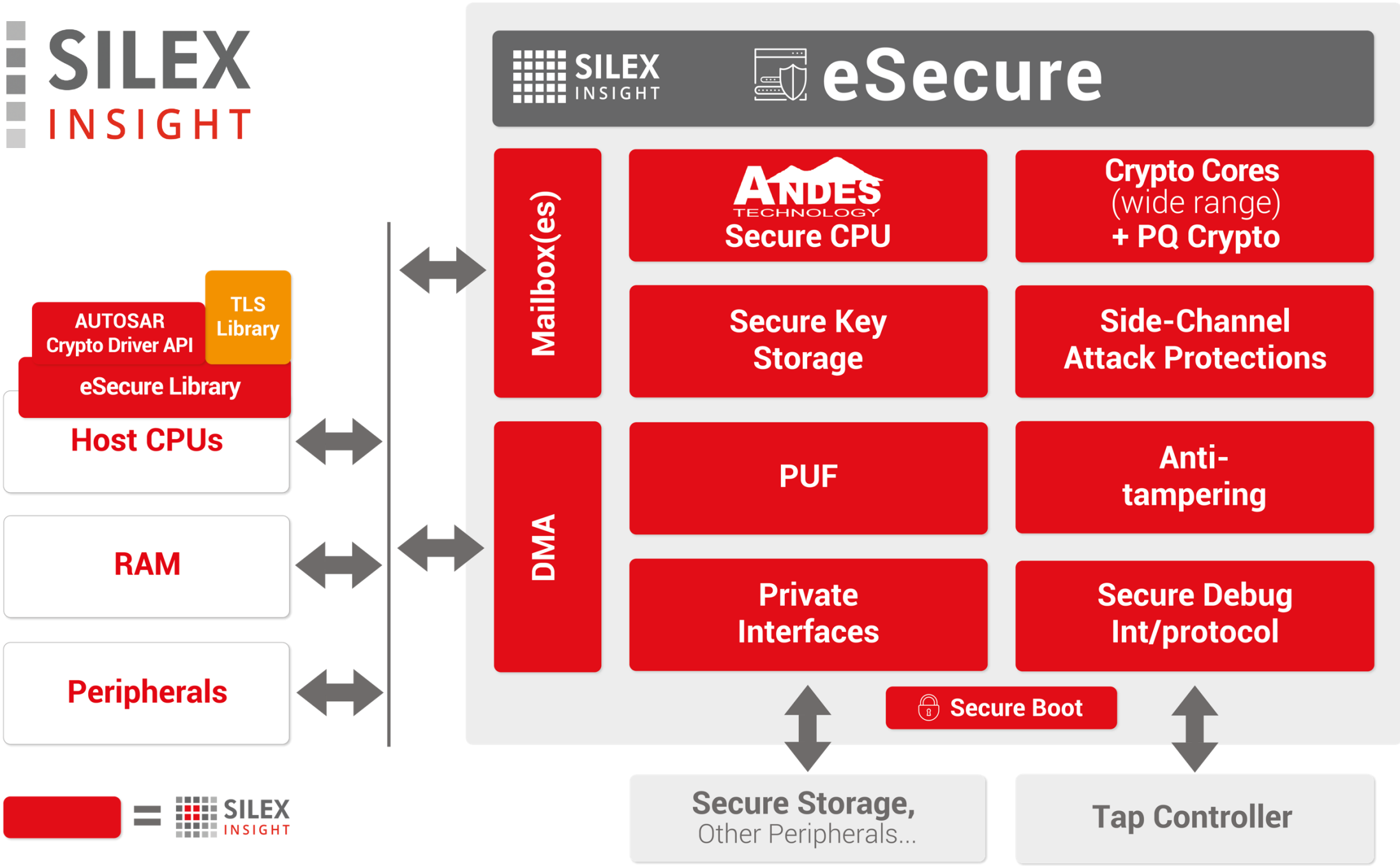
SILEX INSIGHT

Securing your device

Summary

- No one single magic solution
- 100% security does not exist
- Is not only about encryption
- Security must be defined at architecture phase
- Security is a hard requirement in IoT

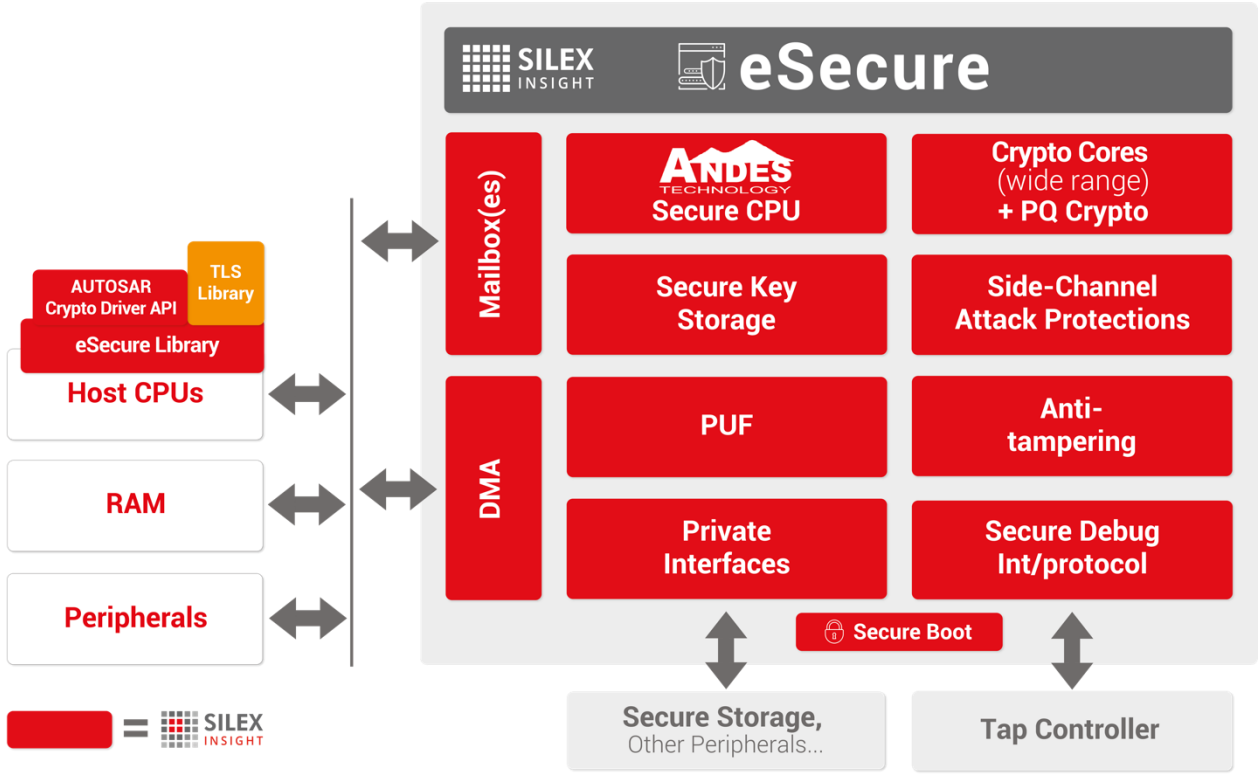
SILEX INSIGHT



eSecure IP

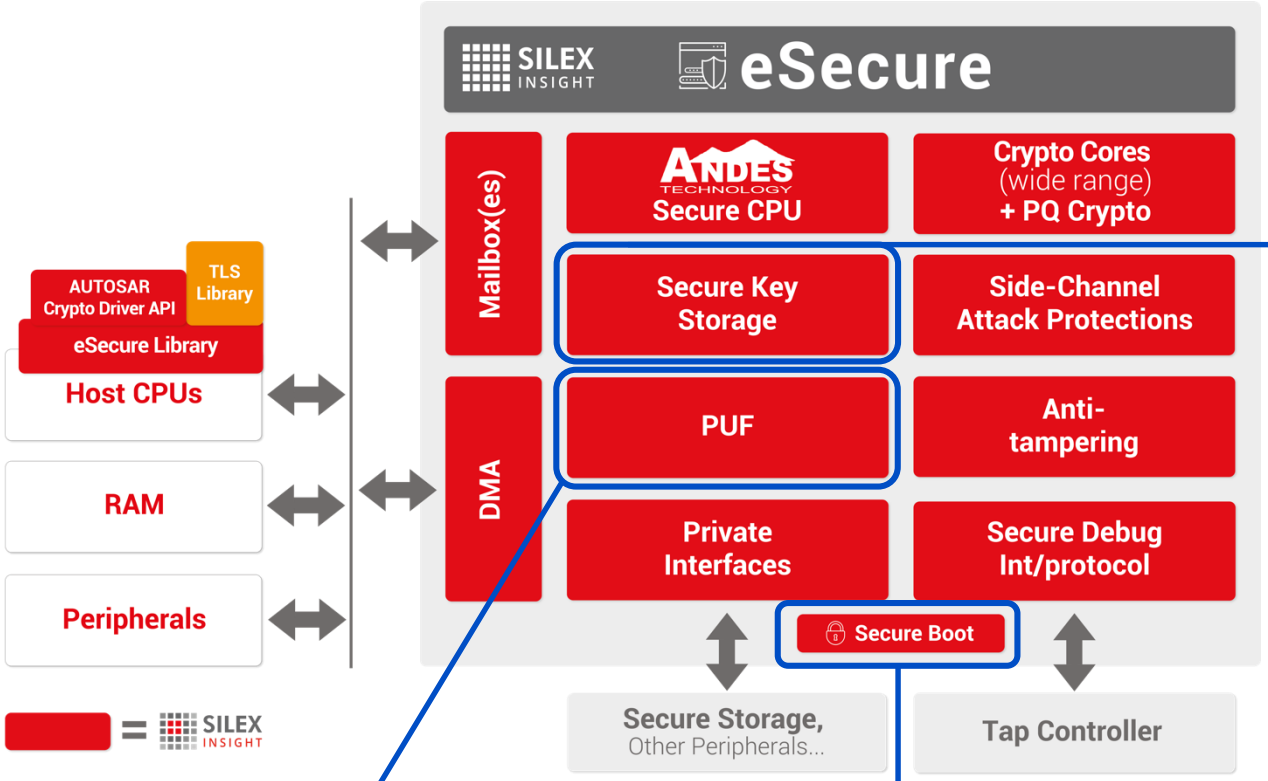
Overview

- Security Enclave/Root-of-trust/HSM
- Hardware isolation between application and secure module
- Flexible and scalable solution using Andes N22 processor



eSecure IP

Key features



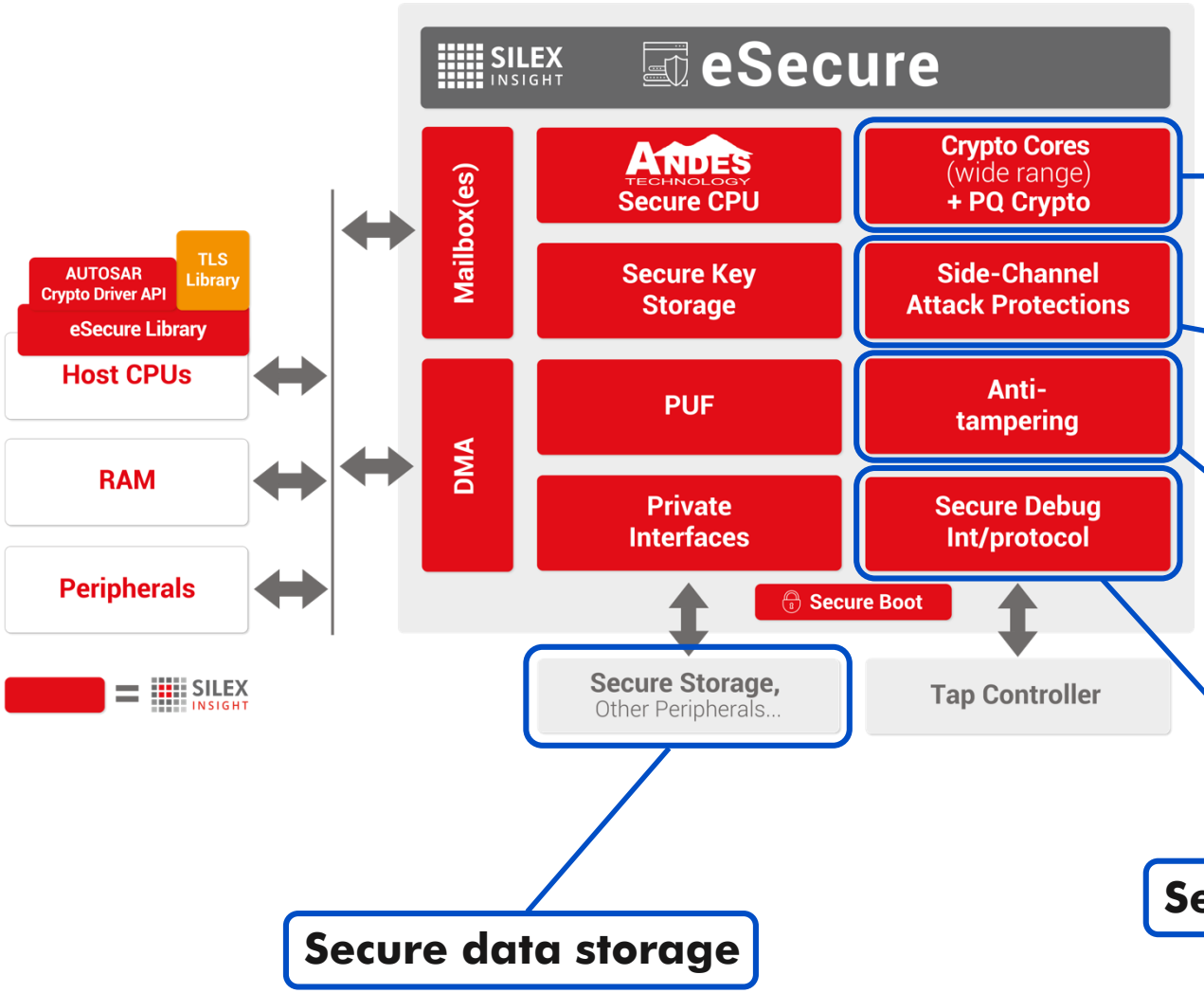
Secure Key Storage
- **Secure Key provisioning**
- **No access to secret by host processor(s)**

Device authentication
- **Unique Key per device**

Secure boot
- **Software and firmware authentication/decryption**
- **Update in the field**

eSecure IP

Key features



Efficient offloading for secure communication (TLS/DTLS, VPN)

Side channel attack protection
- **Anti–tampering mechanism**
- **Erasing of secrets**

Logging of tampering

Secure debugging

Secure data storage

SILEX INSIGHT

eSecure IP

Crypto offloading

- 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/ZUC
- Post-quantum cryptography (PQC) algorithms also available

SILEX INSIGHT

eSecure IP

Certification

- NIST CAVP certificate available for all relevant algorithms
  - https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=31138
- Up to FIPS 140-2 level 3 certification achieved
- PCI DSS certification for payment card industry
- OSCCA certification for Chinese market
- Suitable for automotive HSM (ISO26262)

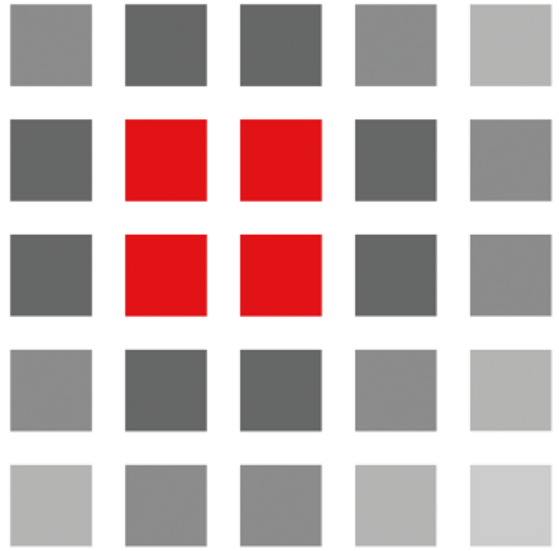
Conclusions

- ***Security required for IoT–*** Think about it at architecture definition level
- ***No system 100% secure*** – Try to discourage the attackers
- ***Lifecycle of your products*** – Needs capability to do SW update
- ***Trade-off*** – cost, power, performance, security

This is Silex Insight

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



SILEX INSIGHT

EMBEDDED IN YOUR FUTURE

www.silexinsight.com

www.silexinsight.com.cn