



Tiempo
SECURE

Securing IoT with a hardware Secure Element

Marc Renaudin - Serge Maginot - TIEMPO



Connected Objects

Securing IoT with a hardware Secure Element

- Introduction
- Securing – Treats – Security Services
- Software and Hardware Architecture
- Key provisionning
- Normalisation
- Conclusion

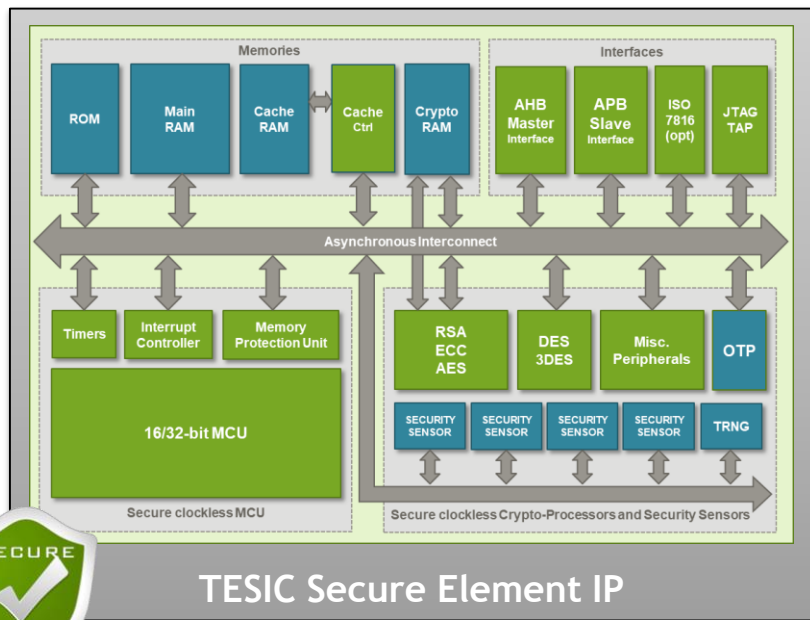


Introduction : Tiempo Secure products and markets

Tiempo security IP and expertise

Tiempo products

Tiempo customers

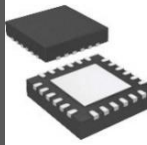


TESIS Secure Element IP

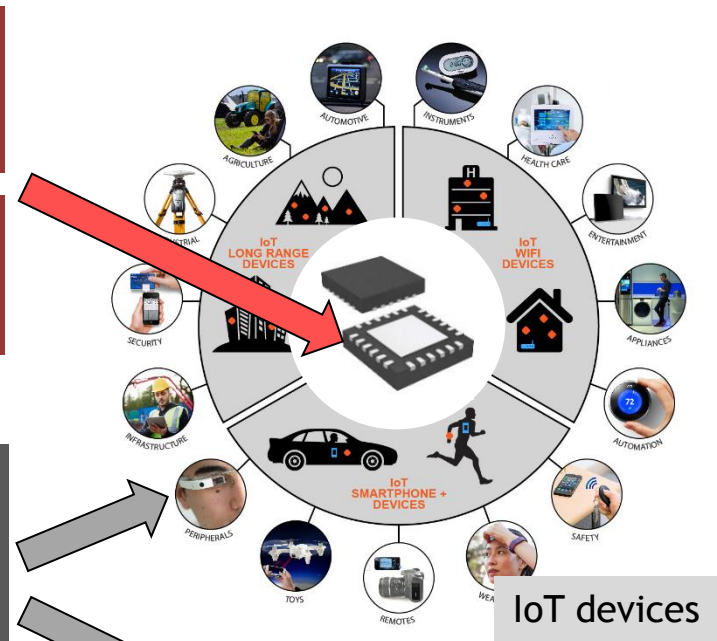


Secure Element Hard IP

Secure Design Services



Certified Secure MCU Chips



smartcards

eGov/eID

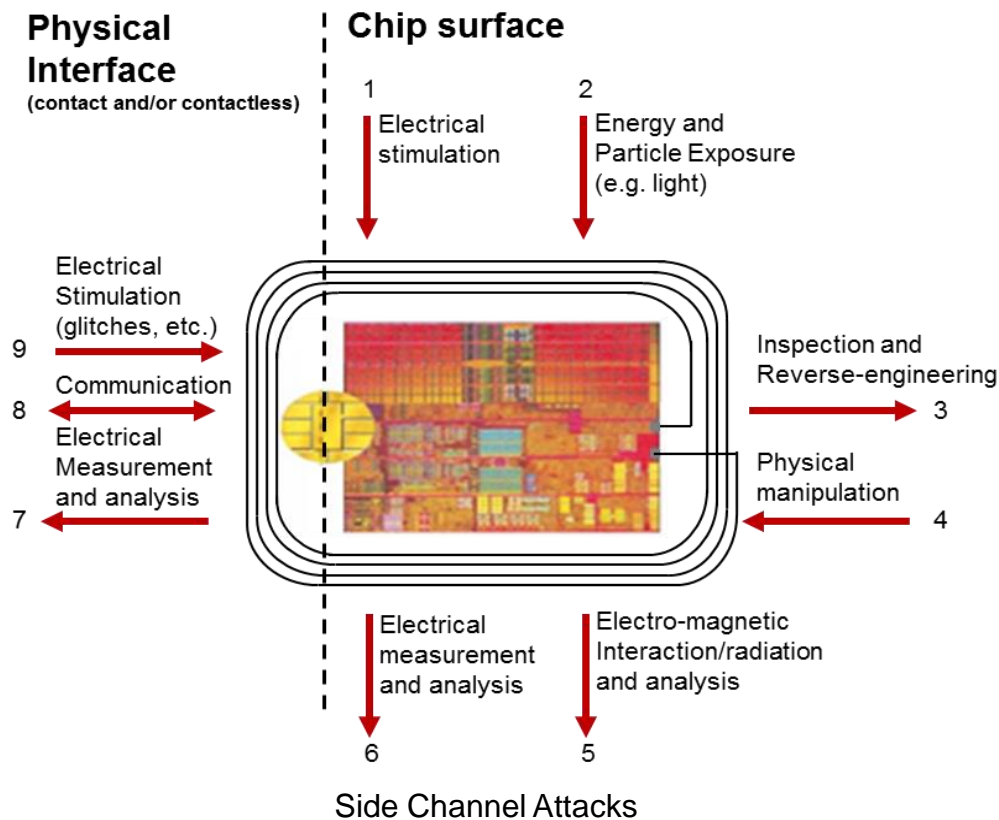


Tiempo security certifications (CC EAL5+, EMVCo)



Securing – Treats – Security Services

- Interaction between the TOE and its outer world
 - Confidentiality, Integrity and Authentication





Leading IoT market requirements to SoCs

- **Connectivity:** SoCs have to be connected + to **communicate**
- **Security:** SoCs have to **resist** today's + future attacks
- **Lifetime:** SoCs have to run **10 years +** on standard batteries
- **Size:** SoCs are inserted into **very small devices**
- **Price:** SoCs have to be very **price competitive**
- **Flexibility:** **One** SoC design should **fit many** solutions/markets



TESIC: secure element IP for secure chips

TESIC is a generic CC EAL5+ certification-ready secure element IP with following USPs:

a. No third-party IP ownership/royalty

- ✓ Proprietary secure microcontroller: CC EAL5+ certified core,
- ✓ Proprietary secure crypto-processors and
- ✓ Proprietary security sensors

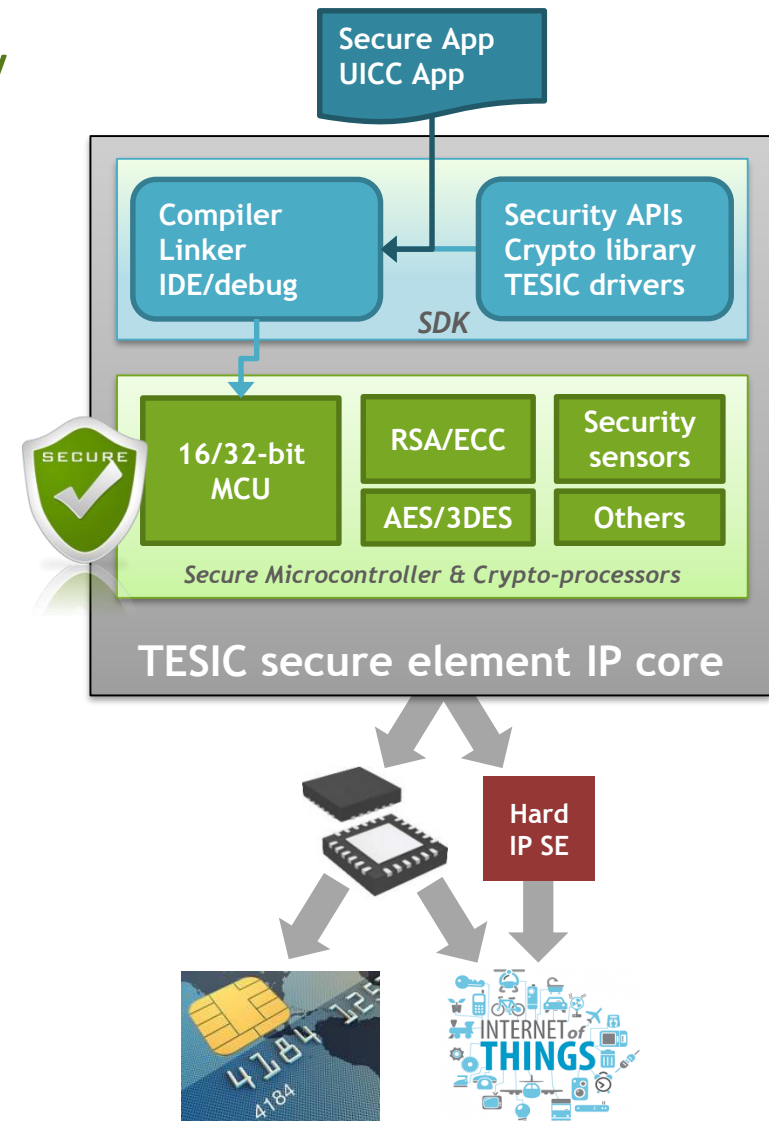
b. Silicon-proven on various geometries

- (130 nm, 110 nm, 55nm, 40nm, 28nm, under preparation: 22nm)
- ✓ Customizable, allowing to target various secure applications
 - ✓ Offers pre-qualified security and outstanding performance

c. Customer-validated SDK

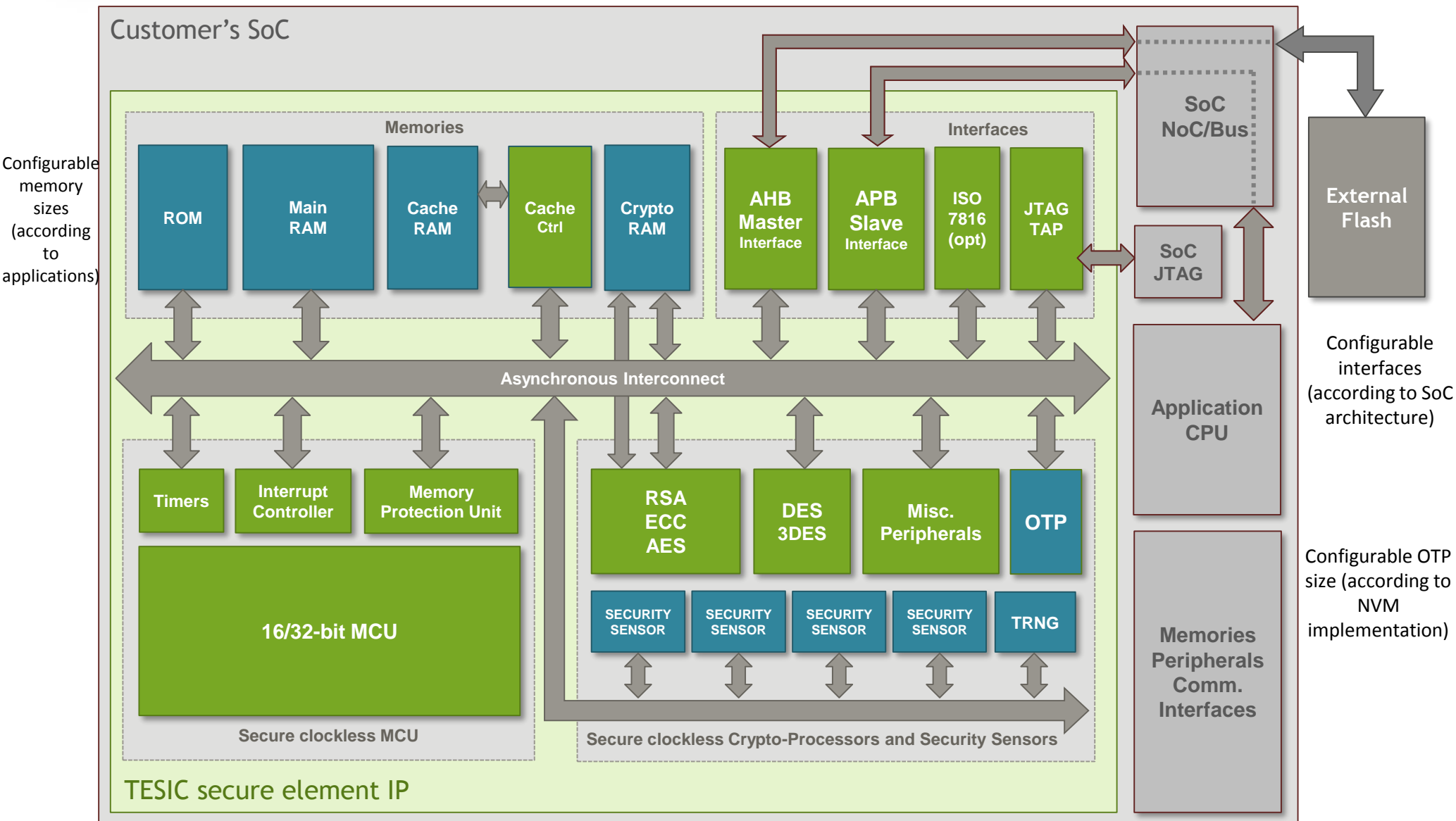
d. CC EAL5+ and EMV-Co certified (TESIC-SC)

- ✓ Cryptographic Library +
- ✓ Secure Boot Loader



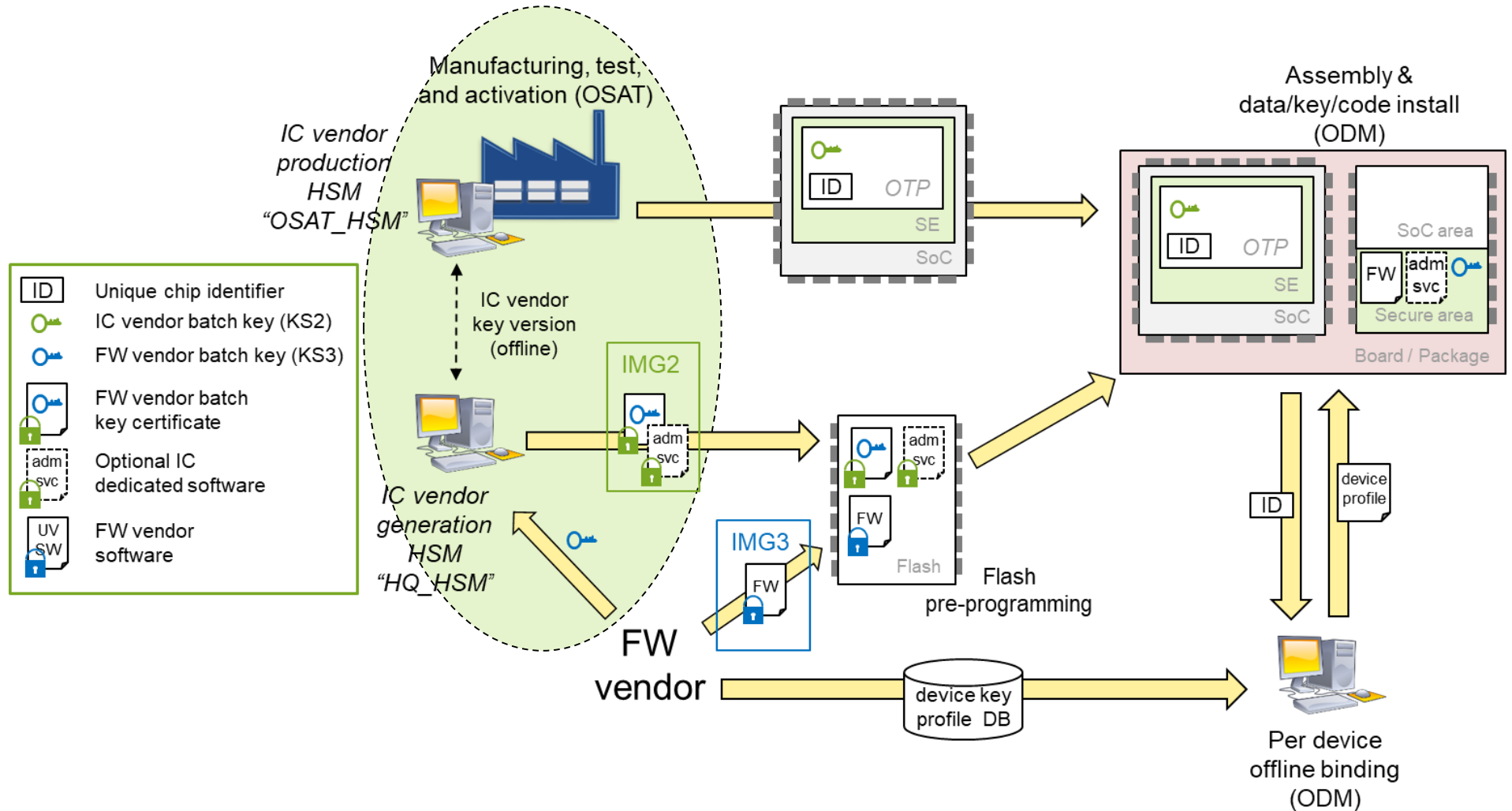


SoC integration of TESIC secure element





Provisioning : HSM setup for TESIC enabled SoCs



Tiempo's CC EAL5+ compliant key management flow (with flash pre-programming)



- **CC EAL5+ and PP0084 Package 2**
 - Common Criteria VAN.5 and DVS.2 => Attacks and Life Cycle
 - Protection Profile Package 2 => Security functions and Software Updates
- **Strong expertise in secure HW and SW developments**
 - State-of-the-art security countermeasures, hardware and software
 - Certified crypto-library and boot loader (protection profile PP0084b)
 - Certified design center and documentation (CC EAL5+ and EMVCo)
- **Tiempo is in constant collaboration with security labs (CESTI) and certification offices (French ANSSI, European Eurosmart/JHAS)**
 - Remains up-to-date regarding the state of the art of physical attacks
 - Innovates with always better/new/patented security countermeasures
- **Participates to working groups on coming EU IoT security standard**





- Tiempo delivers a Secure Hard IP to secure IoT devices
 - That is certified at the right level (level of attacks and life cycle)
 - That enable to secure IoT devices (Authentication, Confidentiality, Integrity)
 - That can be integrated within customer's SoC

- Tiempo delivers a complete service to secure IoT devices
 - Provisioning and key management
 - HSM usage in the life cycle

- Tiempo has partnerships and collaborative projects in the IoT markets
 - Lora/Sigfox/LTE-M/NB-IoT/5G
 - SECURIOT
 - SECURE-IP