TRUSTED OBJECTS

LoRaWAN® Security

EU Cybersecurity Act impact

LoRaWAN®

Creating Valuable IoT Connections

Agenda

- EU Cybersecurity Act : overview & key points
- Why EU Cybersecurity certification schemes?
- EU Cybersecurity: security assurance levels
  - Description of the 3 security grades
  - Characteristics of the EU cybersecurity certification schemes
  - Public and private initiatives
- EUROSMART IoT device security certification scheme
- LoRaWAN security positioning against Cybersecurity Act certifications
- Take away

Trusted Objects at a glance

Trusted Objects is a mission-driven company established **to change the face of IoT security** by enabling best practices security solutions to protect the whole IoT ecosystem.

- Independent company founded in 2014 by industry experts.
- Expertize in **cybersecurity technologies for Industrial IoT applications**, including secure embedded software & libraries, secure connectivity stacks, secure design services, personalization & provisioning solutions.
- Global footprint with presence in Europe, Asia (offices in Singapore and Bangalore).
- Solid technical and financial background.

Security is in the DNA of the company

EU Cybersecurity Act – Overview 1/2

- In April 2019, the European Parliament has approved a new cybersecurity regulation, the Cybersecurity Act.
- The Cybersecurity Act does cover networks security, information security and devices security (ICT products or services)
- Under the regulation, the Commission is empowered to adopt European cybersecurity certification schemes, including IoT devices.
- Unification of national certification schemes.

The European cybersecurity certification is completely separate and independent of the LoRaWAN® certification

EU Cybersecurity Act – Overview 2/2

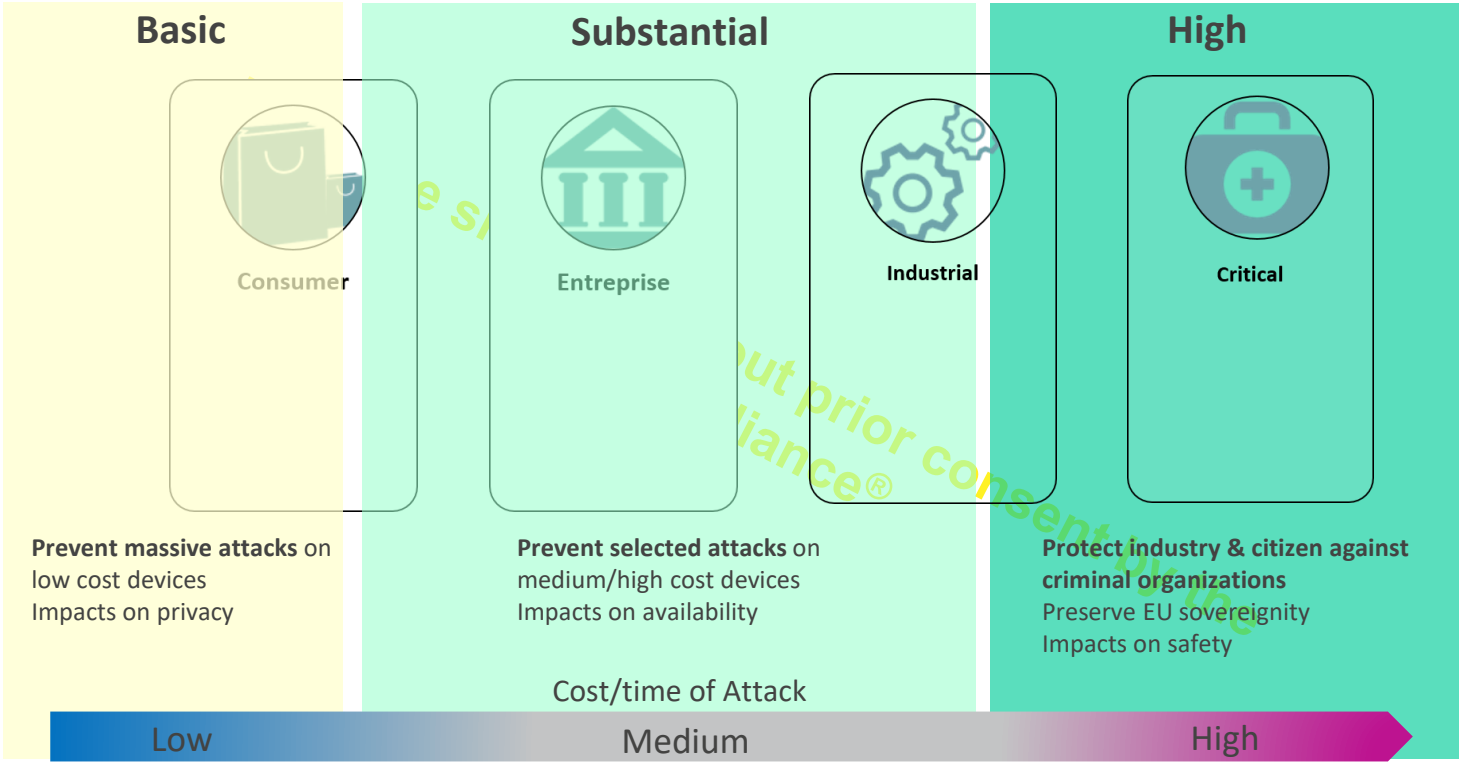
- Key elements of the cybersecurity certification schemes :
  - The new certification schemes will initially be voluntary.
  - The schemes and certification issued for products and services will specify 3 different assurance levels: basic, substantial and high.
  - “Security by design” approach at the heart of all projects.
  - EU Member states will establish penalties for infringing European cybersecurity certification schemes.

CERTIFICATION gives TRUST !

- "**TRUST** should be further **strengthened** by offering information in a **transparent** manner on the **level of security** of ICT products, ICT services and ICT processes..."
- "An **increase in trust** can be facilitated by **Union-wide CERTIFICATION** providing for **common cybersecurity requirements** and **evaluation criteria** across national markets and sectors."

Cybersecurity Act –Section (7)

EU Cybersecurity certification schemes: security assurance levels



Source: Eurosmart

Characteristics of the EU cybersecurity certification schemes

Assurance Level « Basic »
Objective: Inform

- Minimize **the known basic risks** of incidents and cyberattacks
- Security guidelines
- Self assessment

Assurance Level « Substantial »
Objective: Protect

- Minimize **the known cybersecurity risks** carried out with **limited skills and resources**
- Security schemes & Pentests
- Certification by CAB (*)

Assurance Level « High »
Objective: Prevent

- Minimize **the risk of state-of-the-art cyberattacks** carried out with **significant skills and resources**
- Security schemes & Pentests
- Certification by CAB (*)

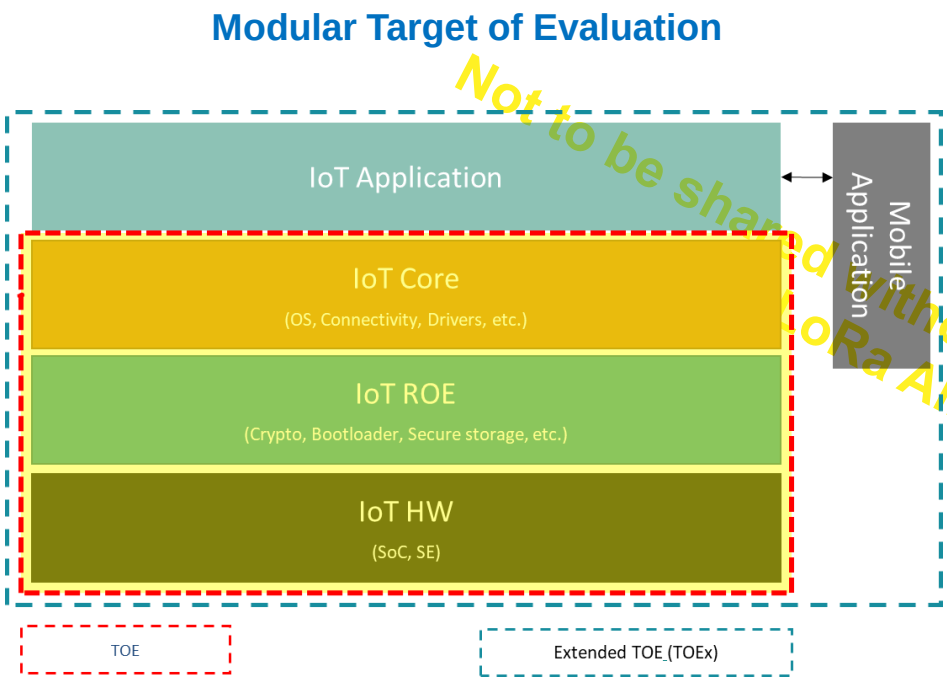
(*): CAB: Conformance Assessment Body

Certification schemes – Public and private initiatives

Scheme Name	Acronym	Key driver	Type of initiative	CSA Level
Eurosmart IoT Scheme		**Eurosmart**	**Private**	**Substantial**
IoT security Architecture		GlobalPlatform	Private	
Platform Security Architecture	PSA	ARM	Private	All
Secure Evaluation Scheme for IoT Platform	SESIP	NXP	Private	All
UL Cybersecuroty Assurance Programme	UL CAP	UL	Private	
Certification Sécuritaire de Premier Niveau	CSPN	ANSSI	Public	High, Substantial
Baseline Certification	BC	BSI	Public	Substantial
Commercial Product Assurance	CPA	CESG	Public	Substantial
Baseline Security Product Assessment	BSPA	NLNCS	Public	Substantial
SOG-IS for IoT		SOG-IS	Public	
LINCE		National Cryptologic Center	Public	High
ETSI TS103 655(Technical Specifications)	ETSI TS103 655	ETSI	ESO	Basic

EUROSMART – The Voice of the Digital Security Industry

EUROSMART - A certification scheme dedicated to IoT devices



Source: Eurosmart

- Not all products require the same level of certification.
- From a full hardware platform with an OS and cloud connectivity to individual components such as a Secure Element, MCU, or MPU.
- Secure evaluation scheme allows integrators to utilize the security testing on the Root-of-trust to enable less complex certification on their layer.

EUROSMART - IoT Device security certification scheme

Eurosmart scheme has been developed to **fulfill the requirements of the European Cybersecurity Certification framework** at the level “substantial”.

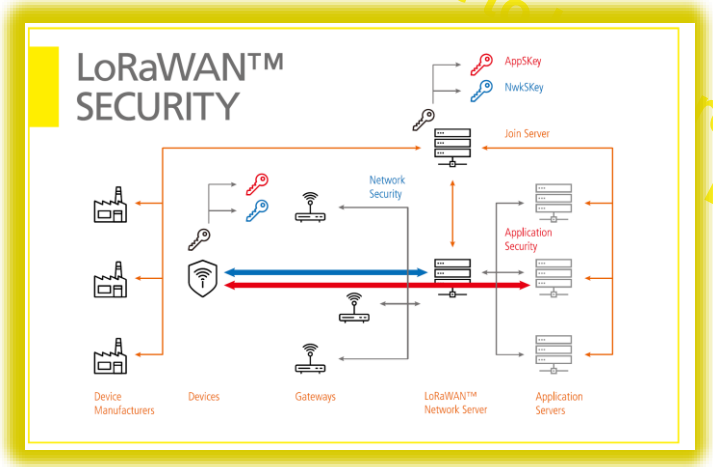
June 2019
Pilots certification phase start!

Security Profile → **Vendor questionnaire** → **Evaluation** → **Certification**

Certification duration is in days

Optimized cost

LoRaWAN® device security



Source: LoRa Alliance™

Physical Security of a LoRaWAN® Device

AppKey and the derived session keys are persistently stored on a LoRa Alliance™ device and their protection depends on the device physical security. If the device is subject to physical threats, keys can be protected in tamper resistant storage (a.k.a. Secure Element), where they will be extremely difficult to extract.

Source: LoRa Alliance™

Threats

- Physical attacks (non invasive/ invasive): key extraction, replay attacks…
- Logical attacks: malware injection, buffer overflows…

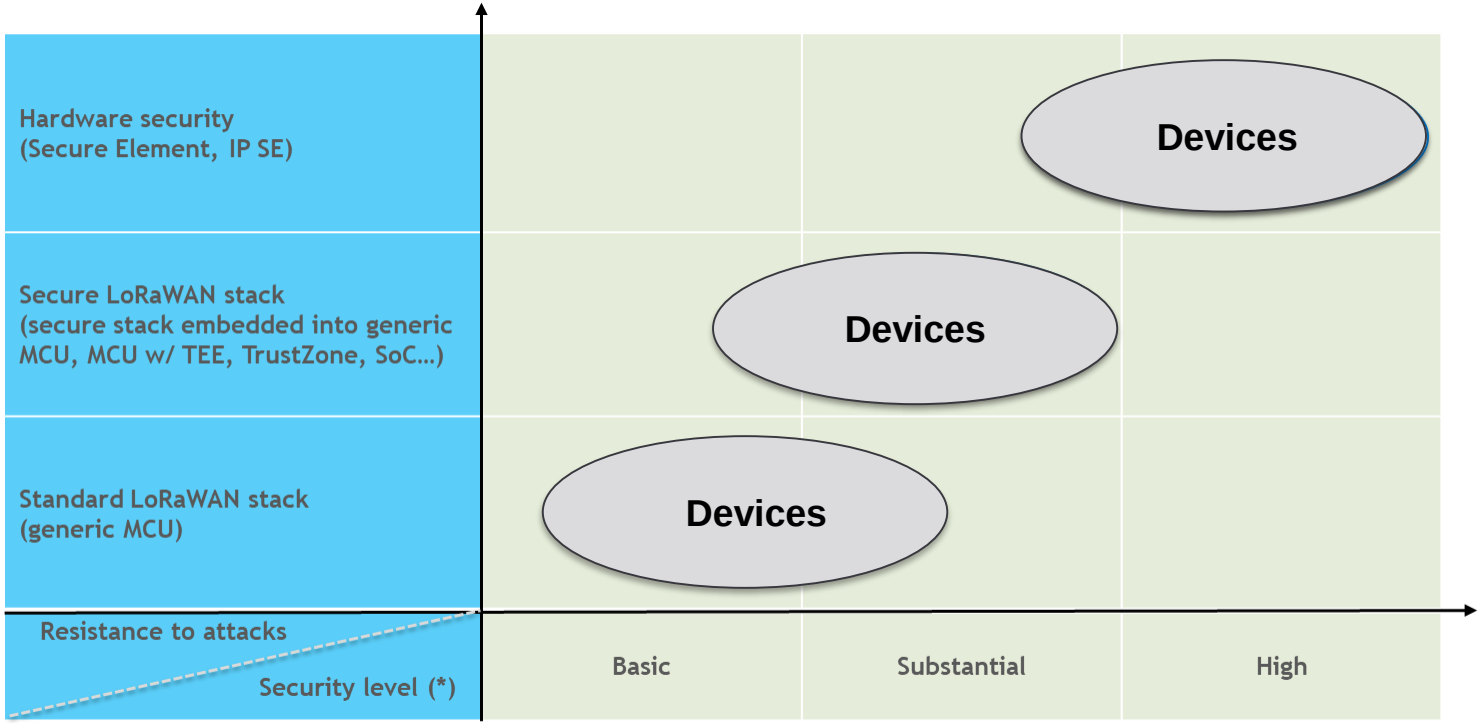
Vulnerabilities

- Unprotected end node
- Unsecured provisioning flow
- Unsecured supply chain

Risks

- Data disclosure or data corrupted
- Usurpation in sending fake commands
- DDoS attacks

Device security against Cybersecurity Act Certification



(*): Cybersecurity Act –Security assurance levels

Take Away

- EU Cybersecurity Act will be the first step of IoT security regulation.
- Security certification to be categorized in 3 levels: basic, substantial, high.
- Substantial and high grades will include security evaluation by CAB, with pentests
- It could lead to achieve security certification for LoRaWAN® devices depending on use case and physical threats.
- We must be prepared based on security principles: secure by design, secure device, secure provisioning, end-to-end security……

LoRaWAN®

Creating Valuable IoT Connections

@LoRaAlliance

linkedin.com/company/loraalliance/

marcom@lora-alliance.com

lora-alliance.org

LoRa Alliance™