EUROSMART

The Voice of the Digital Security Industry

E-IoT-SCS
Eurosmart
IoT Device Certification Scheme

Roland Atoui

Managing Director - Red Alert Labs

EUROSMART
The Voice of the Digital Security Industry

The Voice of the Digital Security industry is an association gathering technological experts in the field of the Digital security

Members are: manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers; Laboratories, Research organizations and Associations.

EUROSMART
The Voice of the Digital Security Industry

Companies

- BACTECH
- business card associates
- FINGERPRINTS
- gemalto a Thales company
- G+D Mobile Security
- IDEMIA augmented identity
- +iD
- IN GROUPE
- TOSHIBA
- infineon
- Linxens crafting the future of connections
- Real Casa de la Moneda Fábrica Nacional de Moneda y Timbre
- NEDCARD
- NXP
- Sanoïa e-health for the real life
- SAMSUNG
- ST life.augmented
- TRUSTED OBJECTS
- WISeKey
- winbond
- INTERNET OF TRUST

Laboratories

- leti ceatech
- KEOLABS
- SERMA TECHNOLOGIES
- brightsight the number one security lab in the world
- Cabinet Louis Reynaud

(TIC) Testing, Inspection, Certification

- SGS
- BUREAU VERITAS
- TRUSTCB TRUST AND VERIFY

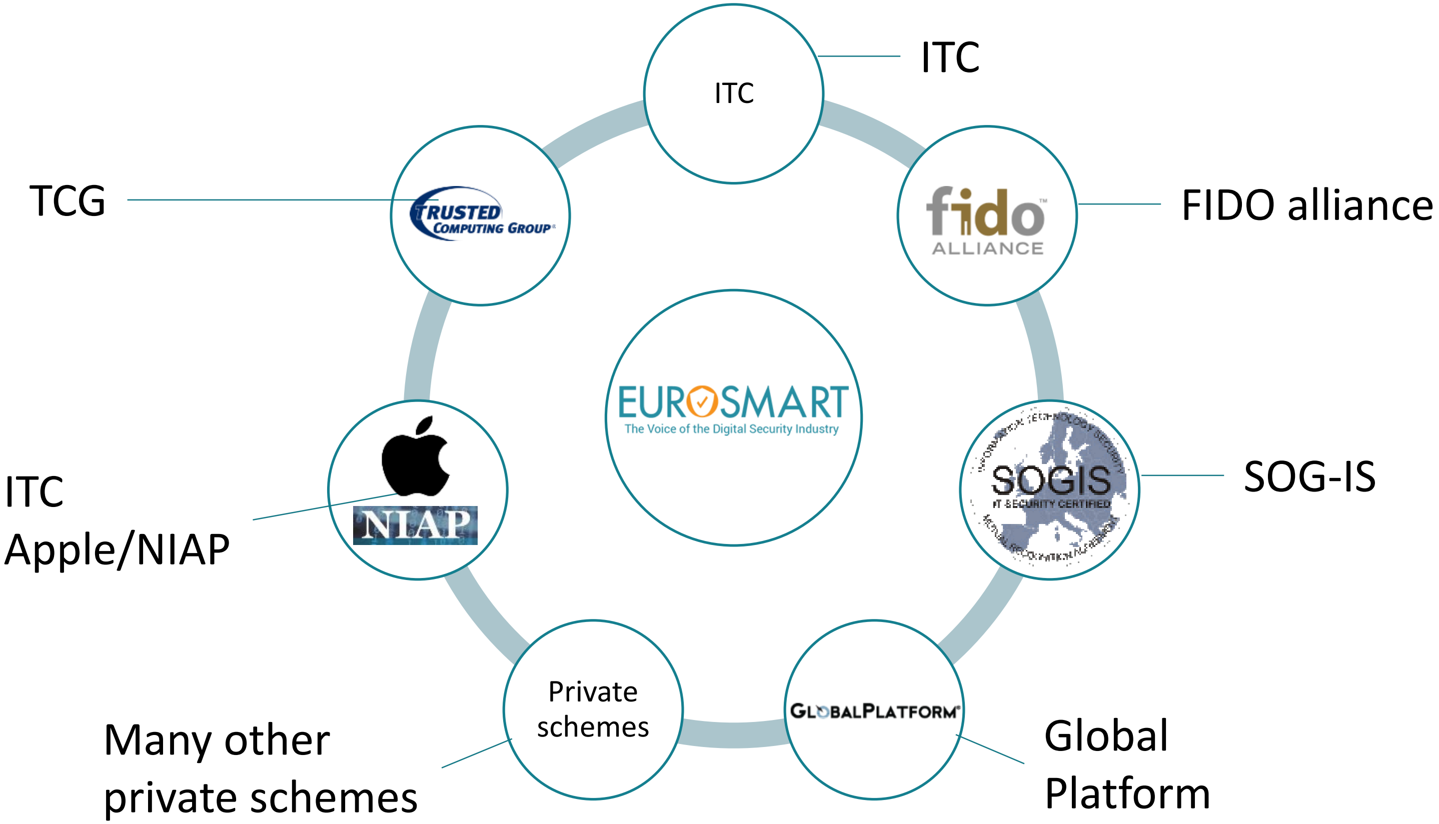
Associations

- SECURED COMMUNICATING SOLUTIONS A WORLD CLASS CLUSTER
- SMART PAYMENT ASSOCIATION

Academics and Research organisations

- Fraunhofer AISEC
- ISEN ALL IS DIGITAL! yncréa

Certification Scheme contribution



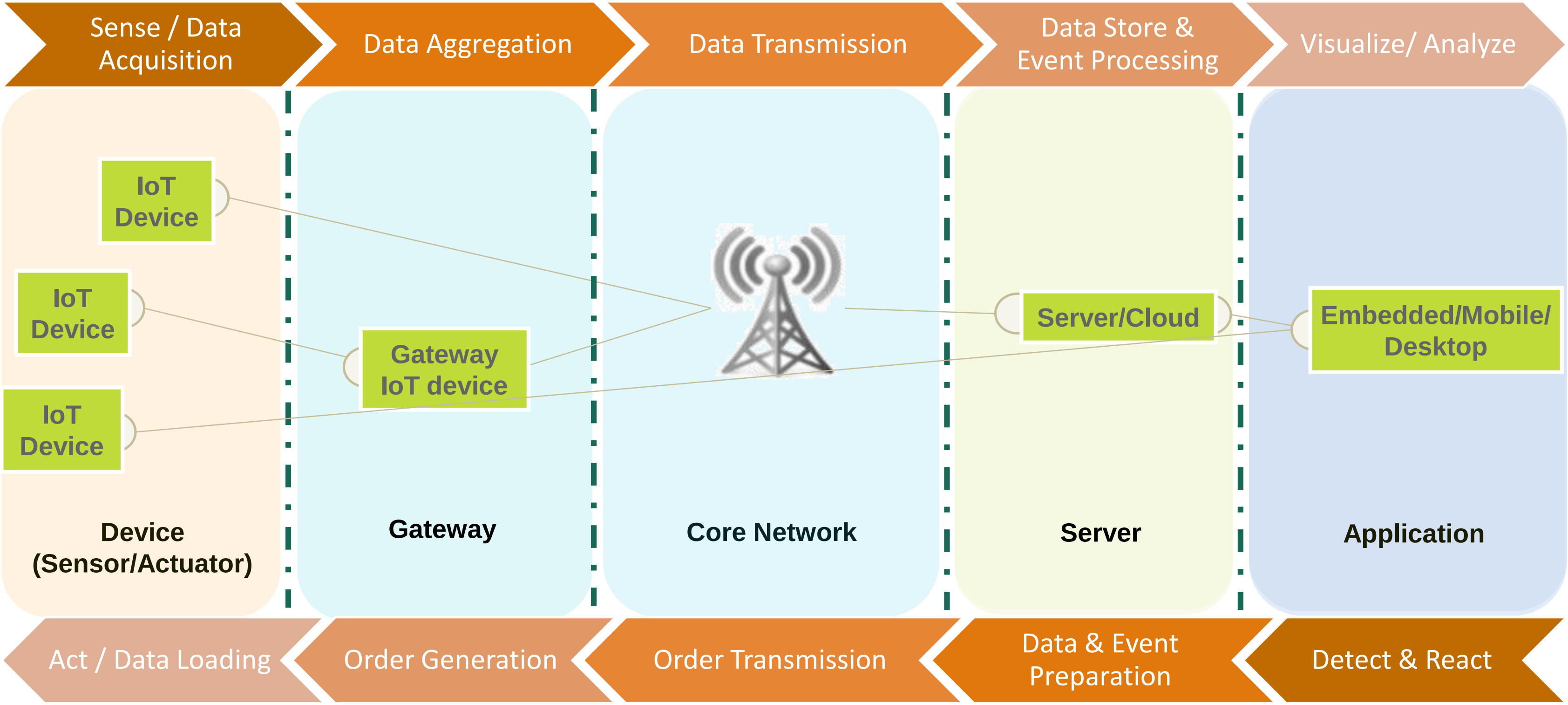
Internet of Things

- **The internet of things**, or IoT, is a system of interrelated computing devices, mechanical and digital machines, with the ability to monitor and transfer data over a network without requiring human-to-human or human-to-computer interaction.
- "IoT since 1996, IoTT since 2018" (the 1st T stands for thinking, for example using AI)

An **IoT Device** is a "Thing":

- **A Hardware** including microcontrollers, microprocessors, mother board, ICs, physical ports.
- **A Software** including an embedded OS, its firmware, programs and applications
- **Sensors** which detect and/or measure events in its operational environment and send the information to other components
- **Actuators** which are output units that execute decisions based on previously processed information

Typical IoT Infrastructure


Sense / Data Acquisition

Data Aggregation

Data Transmission

Data Store & Event Processing

Visualize/ Analyze

Device (Sensor/Actuator)

Gateway

Core Network

Server

Application

Act / Data Loading

Order Generation

Order Transmission

Data & Event Preparation

Detect & React

EUROSMART
The Voice of the Digital Security Industry

A lot of Benefits … with high security risk !

~50 billions in 2020

Fraud & Misuse

Hundreds of millions of internet-connected TVs are potentially **vulnerable to click fraud, botnets, data theft and even ransomware.**

Smart toasters are used as botnets to **get access to your Facebook account or trigger your webcam'.**

Privacy

Hackers have broken into the massive hospital network of the University of California, Los Angeles, **accessing computers with sensitive records of 4.5 million people.**

Data volumes are increasing so fast so that vendors and businesses lack the time to protect it properly.

Safety

Potentially **deadly vulnerabilities** in dozens of devices such as insulin pumps and implantable defibrillators.

Taking control of someone's car sounds like great way of commuting the perfect murder, but, did you know that its possible to hack into your heart and make it explode?

.

PRESSURE IS RISING…

“in 2017, 8.4 B connected devices, 63% CE products, used in smart home – worldwide” (GARTNER)

“CAN I INTEREST YOU IN A FIREWALL FOR YOUR TOASTER?”

“510 M consumer in the European Economic Area are the weakest buyers for IoT/IoTT products, systems and services”

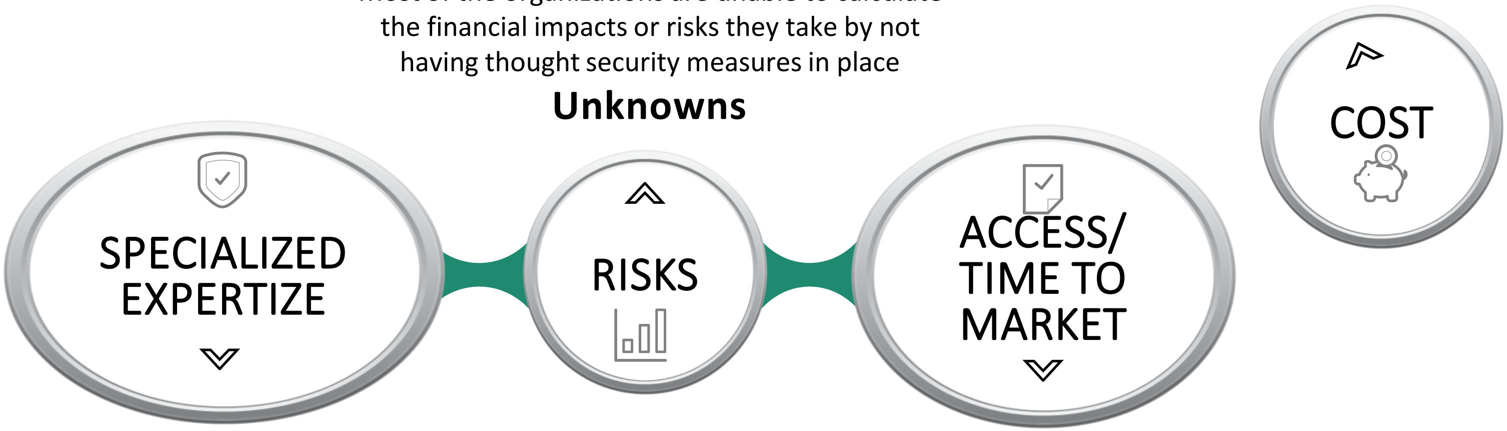
Vendors Problems !

Consumers would always favourite the nice features over security features in a connected product meaning there is no incentive to spend extra money on secure products. A big part of IoT devices cannot support high security development costs for that reason.

Lack of Incentive & Awareness

Most of the organizations are unable to calculate the financial impacts or risks they take by not having thought security measures in place

Unknowns



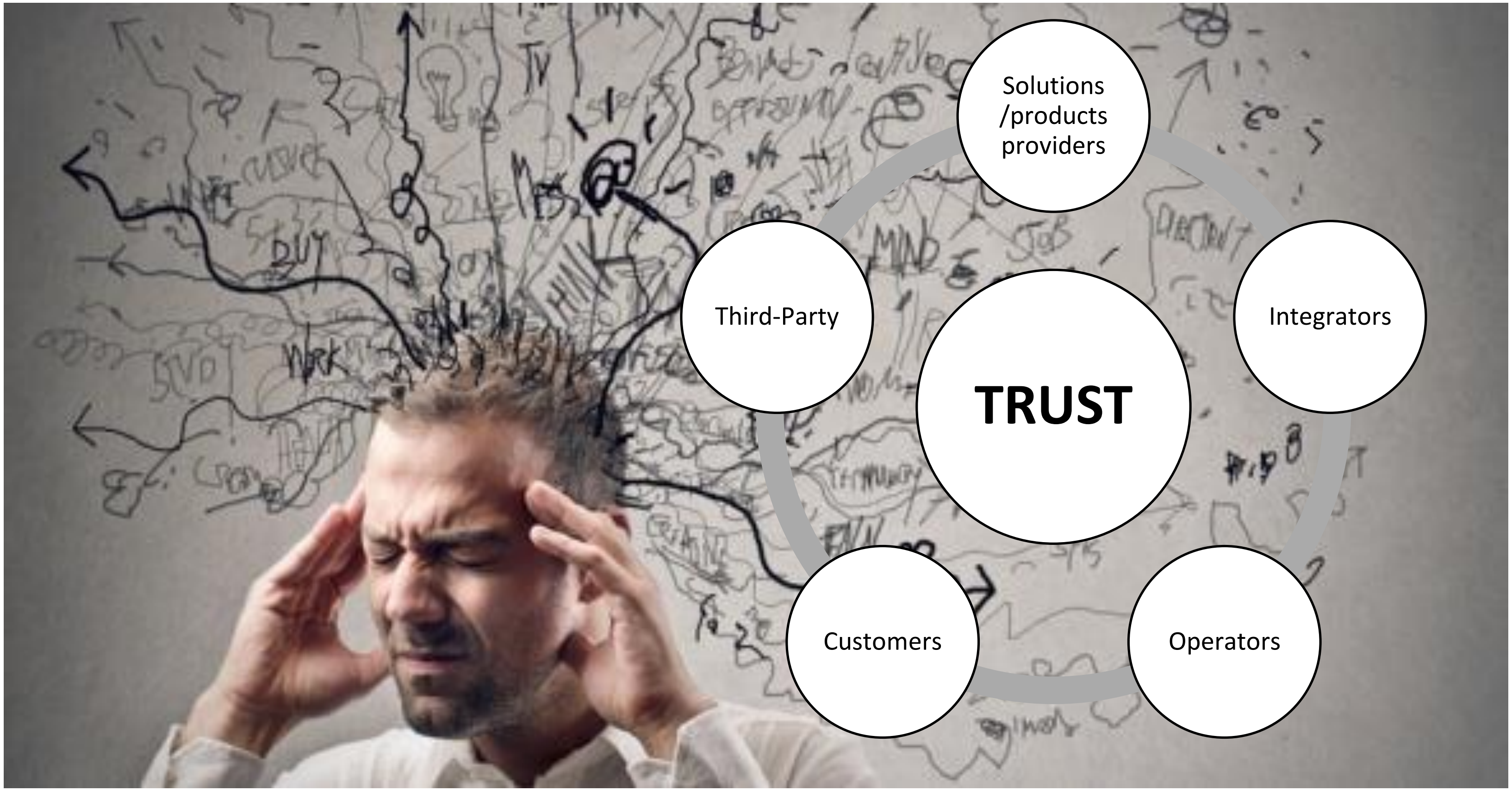
Lack of Security Experts

35% of IoT manufacturers are experiencing shortage of specialized security experts in their organizations as a key challenge to securing IoT products

Compliance & Regulations vs. TTM

All organizations have set priorities to focus on there own market value and loses too much time thinking up security, trying to meet security requirements and regulations set for each vertical. They often fail in meeting TTM

Users/Service Providers Problem !



CERTIFICATION → TRUST

http://www.flickr.com/photos/lwr/

“**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)

WITH THE NEW EU CSA REGULATION WE NEED A NEW CERTIFICATION SCHEME TO TACKLE :

- **Cost, time, validity**
  - Can’t be applied to the 50 Billion IoT product market ! Not enough resources to do that…
- **Subjective**
  - What is the credibility of the evaluation lab/pentester/etc. ?What does secure mean? Can we compare more or less secure products?
- **Scope**
  - Silo Approach - they often cover part of the problem, specific to an industry (banking, ID) but security & privacy is now a concern of every business and citizen.
- **Poor Security Definition**
  - There is no common and holistic approach to define security requirements per profile taking into account the threat model & risks due to the intended usage

AT EUROSMART WE HAVE PREPARED :

Eurosmart IoT Device Security Certification Scheme

E-IoT-SCS

E-IoT SCS

The scope of this certification scheme is the **IoT device** with a focus on the **Substantial** security assurance level as defined by the **Cybersecurity Act**.

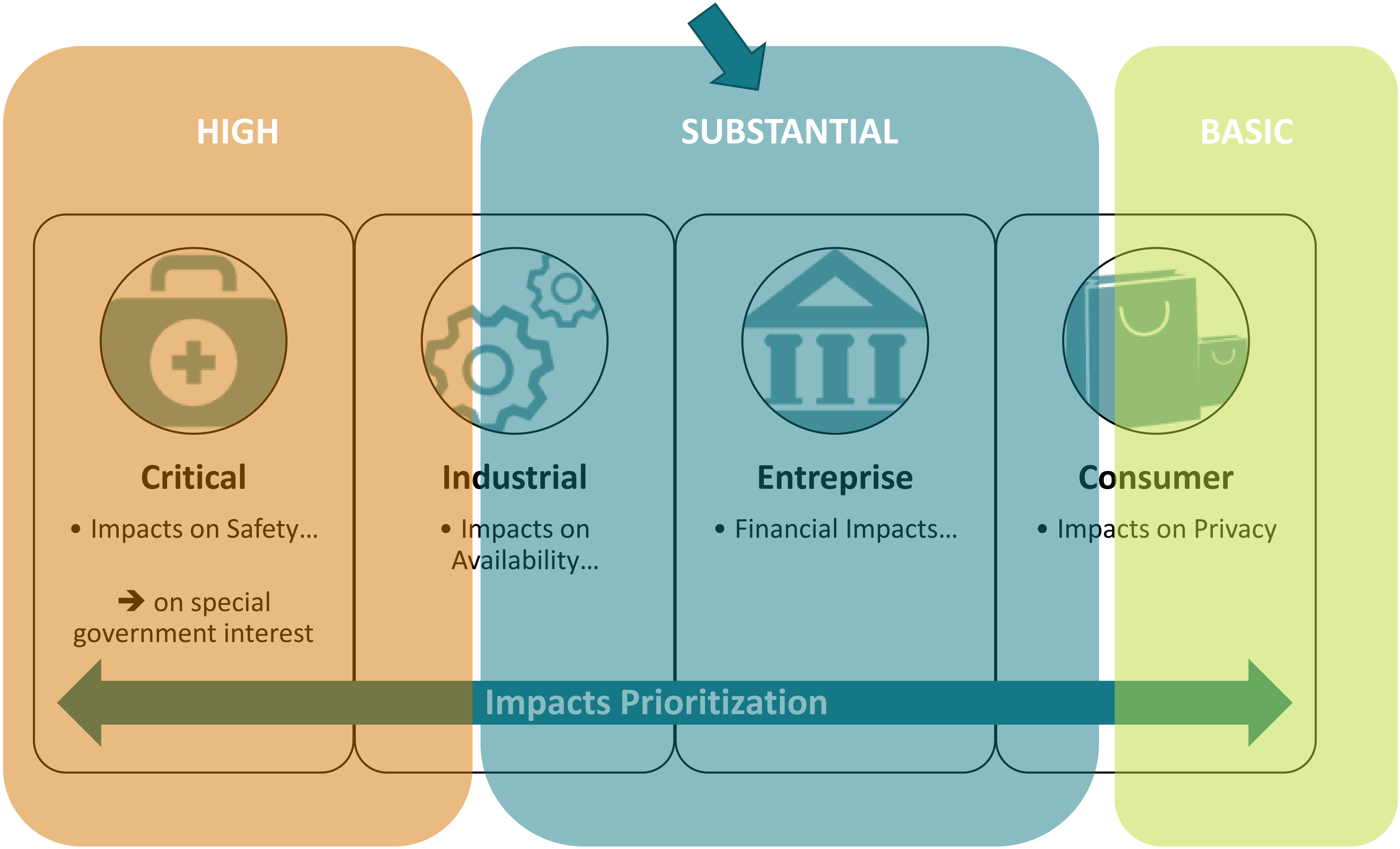
The purpose is to ensure that IoT devices certified under this scheme comply with **specified requirements supported by the industry** with the aim to protect the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions or services offered by, or accessible via IoT devices **throughout their life cycle**.

EUROSMART
The Voice of the Digital Security Industry

3 Security Assurance Levels – Focusing on Substantial

- **Basic**
  - Minimize the known basic risks of incidents and cyberattacks
- **Substantial**
  - Minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources
- **High**
  - Minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources

RISK-BASED IoT MARKET VERTICALS



HIGH

SUBSTANTIAL

BASIC

Critical

- Impacts on Safety…

➔ on special government interest

Industrial

- Impacts on Availability…

Entreprise

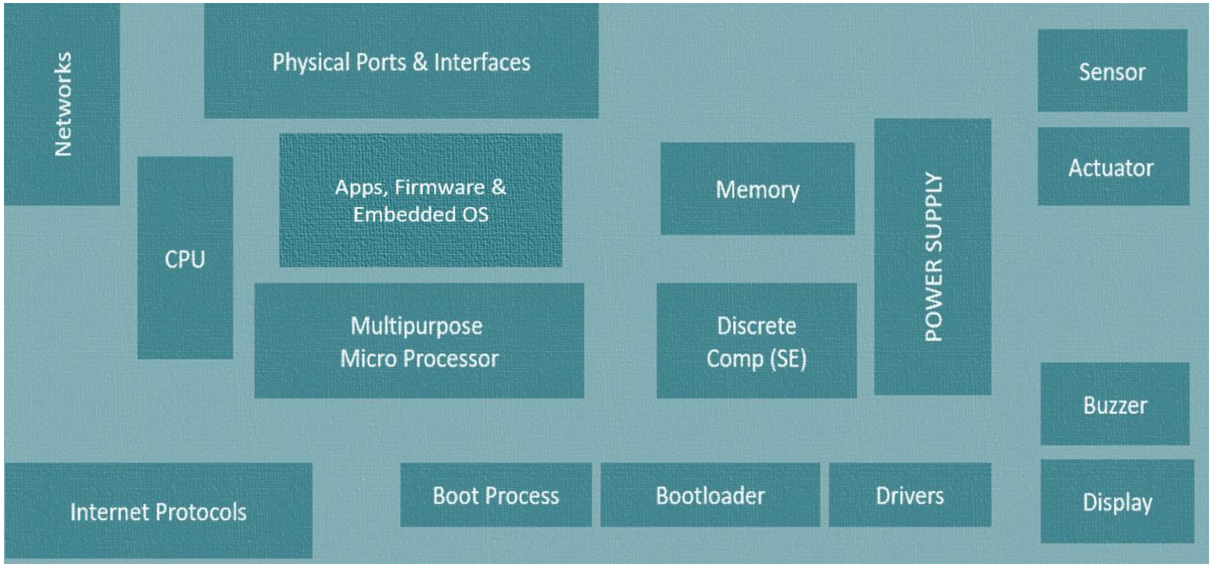
- Financial Impacts…

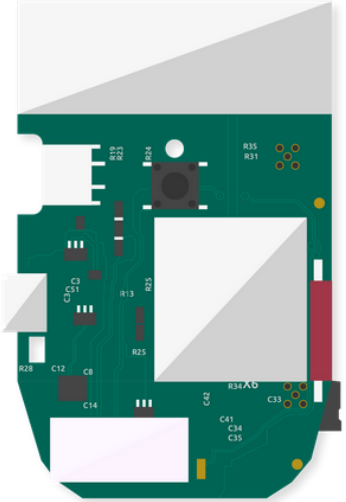
Consumer

- Impacts on Privacy

Impacts Prioritization

Multi-Sensor – Sigfox





Custom antenna

Great performance for all Radio Configurations

250mAh battery

Enough for several months of lifetime (depending on the use case)

Micro-USB port

Recharge the device and dump firmware

Central RGB LED

Improves user experience

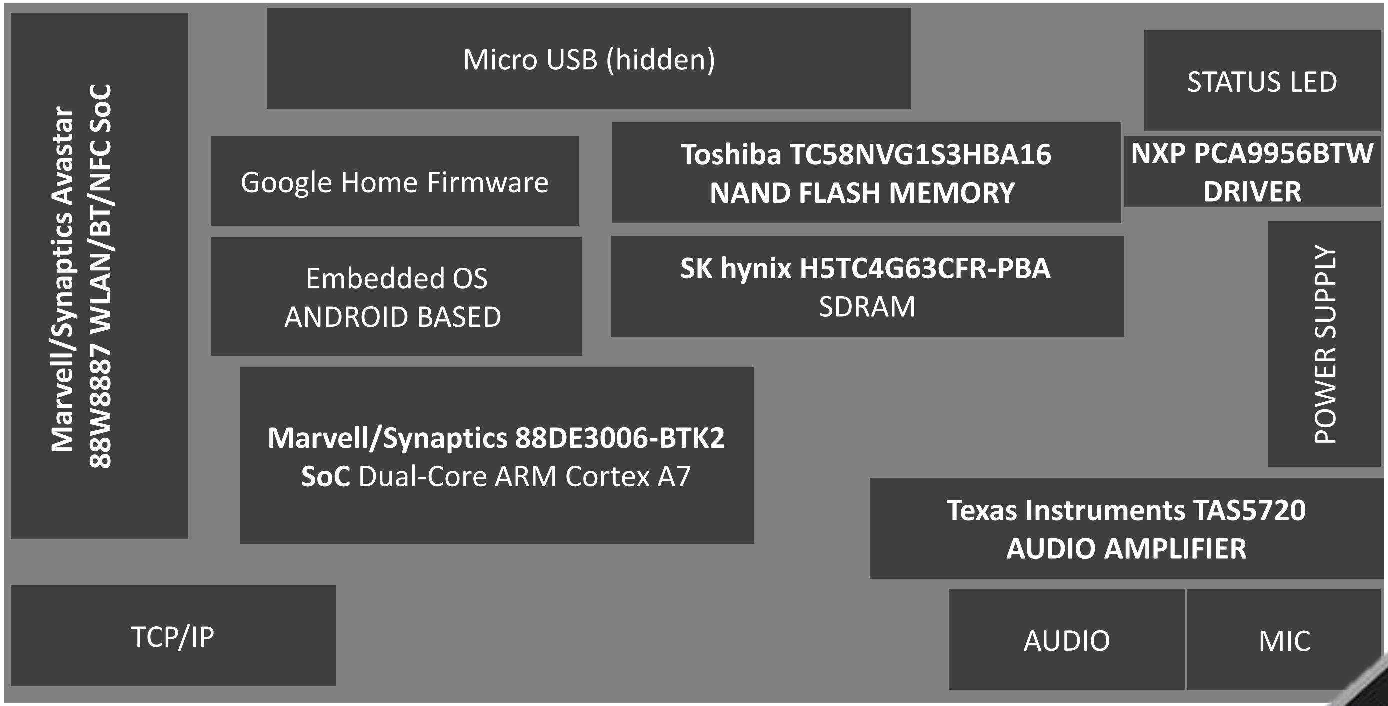
STM32 micro-controller

Controls the device

TI CC1125 radio transceiver

The core of the unique multi-RCs RF design

SMART SPEAKER - Wifi



Marvell/Synaptics Avastar 88W8887 WLAN/BT/NFC SoC

Micro USB (hidden)

STATUS LED

Google Home Firmware

Toshiba TC58NVG1S3HBA16 NAND FLASH MEMORY

NXP PCA9956BTW DRIVER

Embedded OS ANDROID BASED

SK hynix H5TC4G63CFR-PBA SDRAM

POWER SUPPLY

Marvell/Synaptics 88DE3006-BTK2 SoC Dual-Core ARM Cortex A7

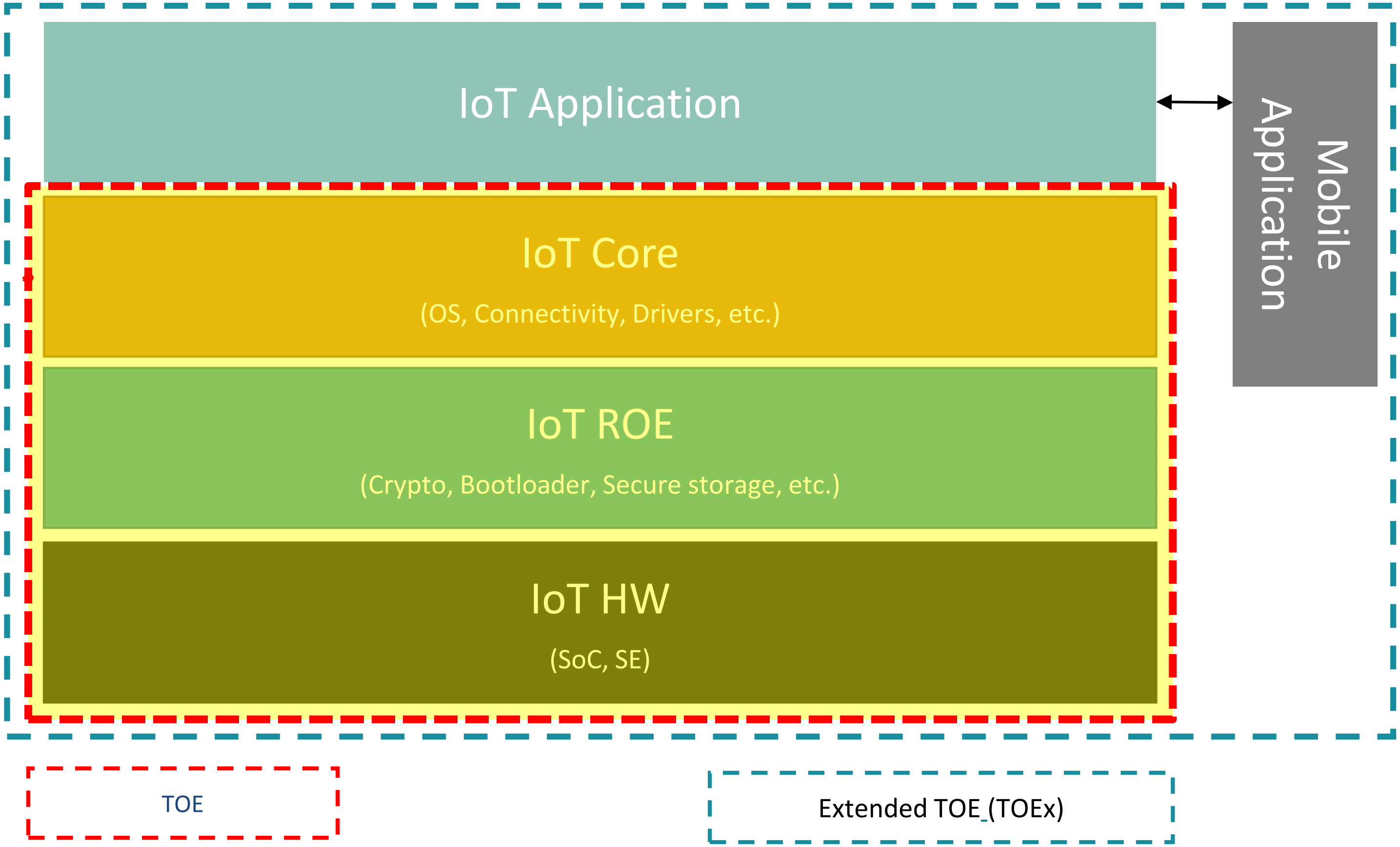
Texas Instruments TAS5720 AUDIO AMPLIFIER

TCP/IP

AUDIO

MIC

MODULAR TOE



IoT Application

Mobile Application

IoT Core

(OS, Connectivity, Drivers, etc.)

IoT ROE

(Crypto, Bootloader, Secure storage, etc.)

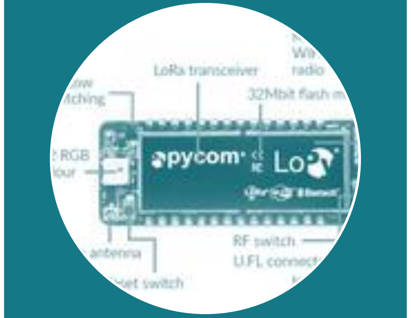
IoT HW

(SoC, SE)

TOE

Extended TOE (TOEx)

TARGETED AUDIENCE



IoT DEVICE VENDOR

IoT PRODUCT VENDOR

IoT SERVICE PROVIDER

IoT DEVICE OWNER

SPONSORS | CONSUMERS

CERTIFICATION PROCESS PHASES

CAB-E = Conformity Assessment Body – Evaluator
CAB-R = Conformity Assessment Body - Reviewer

…..CAB-E&R…… ….CAB-E…… …………………CAB-R………………… …………CAB-E&R…………

SELECTION

- Planning and preparation activities
- CABs Selection
- Specification of requirements
  - *e.g. normative documents, Security Profile, and sampling, as applicable*

DETERMINATION

- Testing
- Inspection
- Design review
- Assessment of services or processes

REVIEW

- Examining the results obtained during the determination stage to establish whether the specified requirements have been met

DECISION

- Granting
- Maintaining
- Extending
- Suspending
- Withdrawing certification

ATTESTATION/MARK

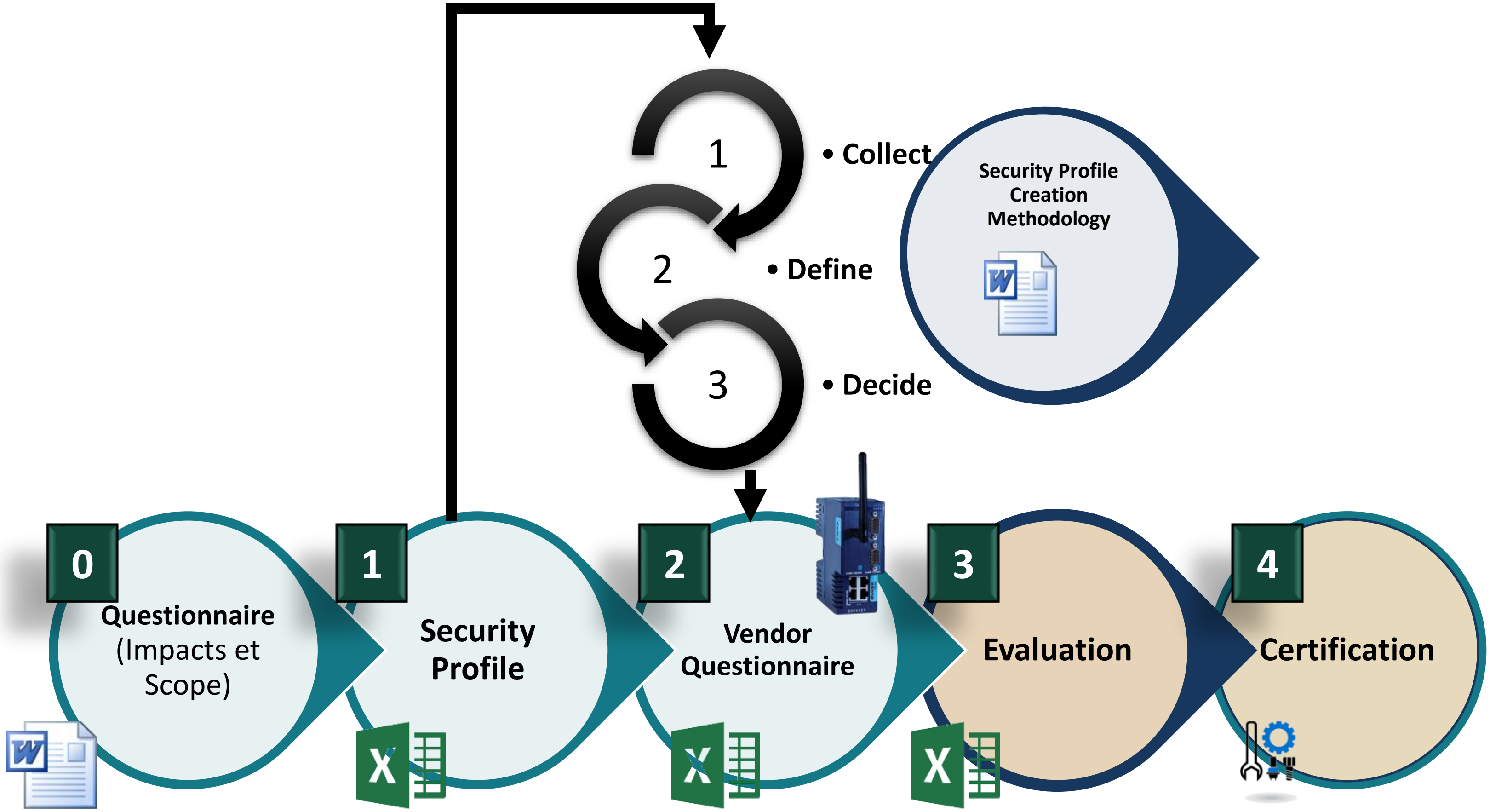
- Issuing a certificate of conformity or other statement of conformity (attestation)
- Granting the right to use certificates or other statements of conformity
- Issuing a certificate of conformity for a batch of products

SURVEILLANCE

- Testing or inspection of samples from the open market
- Testing or inspection of samples from the factory
- Assessment of the production, the delivery of the service or the operation of the process
- Monitoring the Certificates

EUROSMART
The Voice of the Digital Security Industry

VENDOR's STEPS



1 • Collect

2 • Define

3 • Decide

Security Profile Creation Methodology

0 Questionnaire (Impacts et Scope)

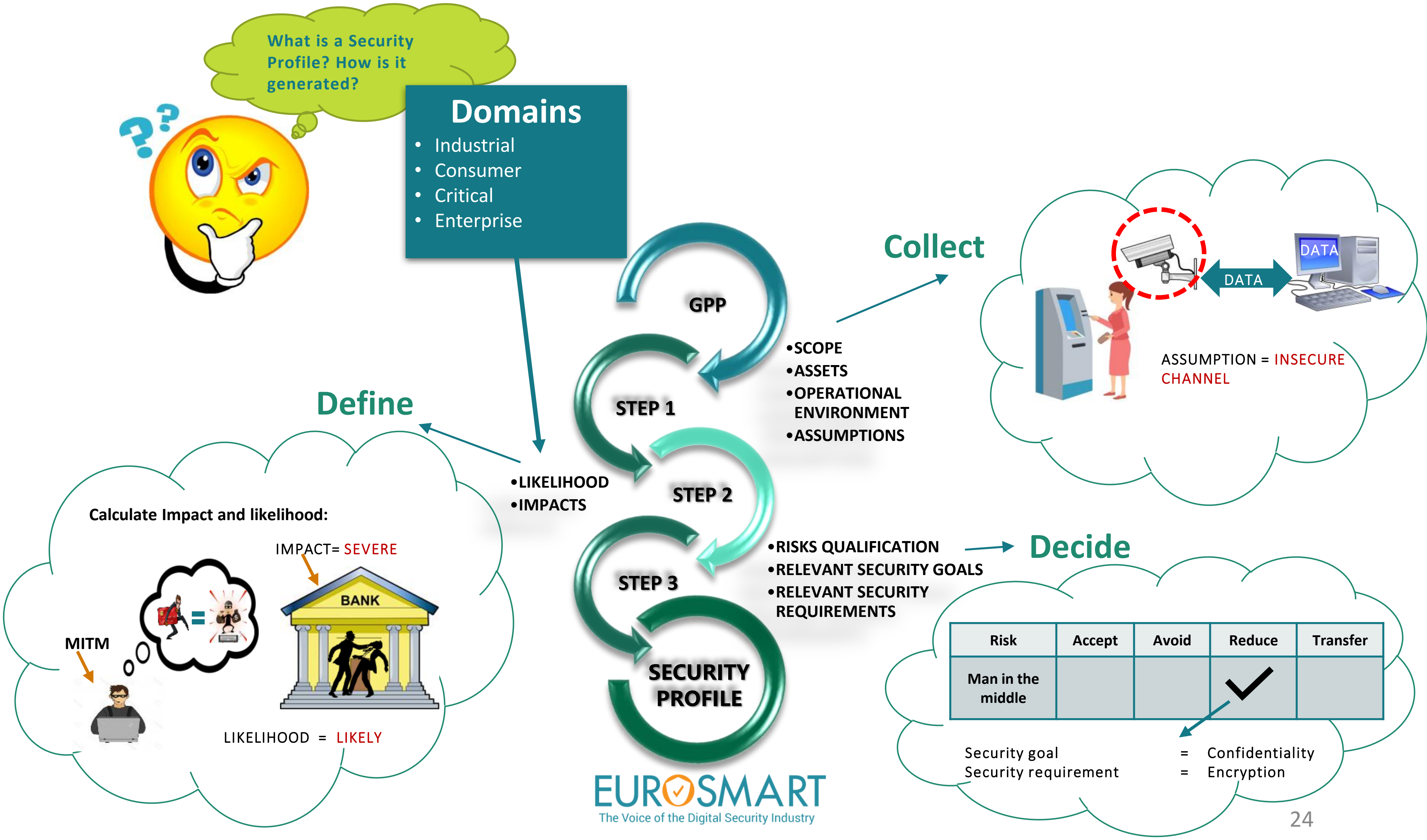
1 Security Profile

2 Vendor Questionnaire

3 Evaluation

4 Certification

SECURITY PROFILE ?



What is a Security Profile? How is it generated?

Domains

- Industrial
- Consumer
- Critical
- Enterprise

GPP

STEP 1

- SCOPE
- ASSETS
- OPERATIONAL ENVIRONMENT
- ASSUMPTIONS

STEP 2

- LIKELIHOOD
- IMPACTS

STEP 3

- RISKS QUALIFICATION
- RELEVANT SECURITY GOALS
- RELEVANT SECURITY REQUIREMENTS

SECURITY PROFILE

Collect

ASSUMPTION = INSECURE CHANNEL

Define

Calculate Impact and likelihood:

IMPACT= SEVERE

LIKELIHOOD = LIKELY

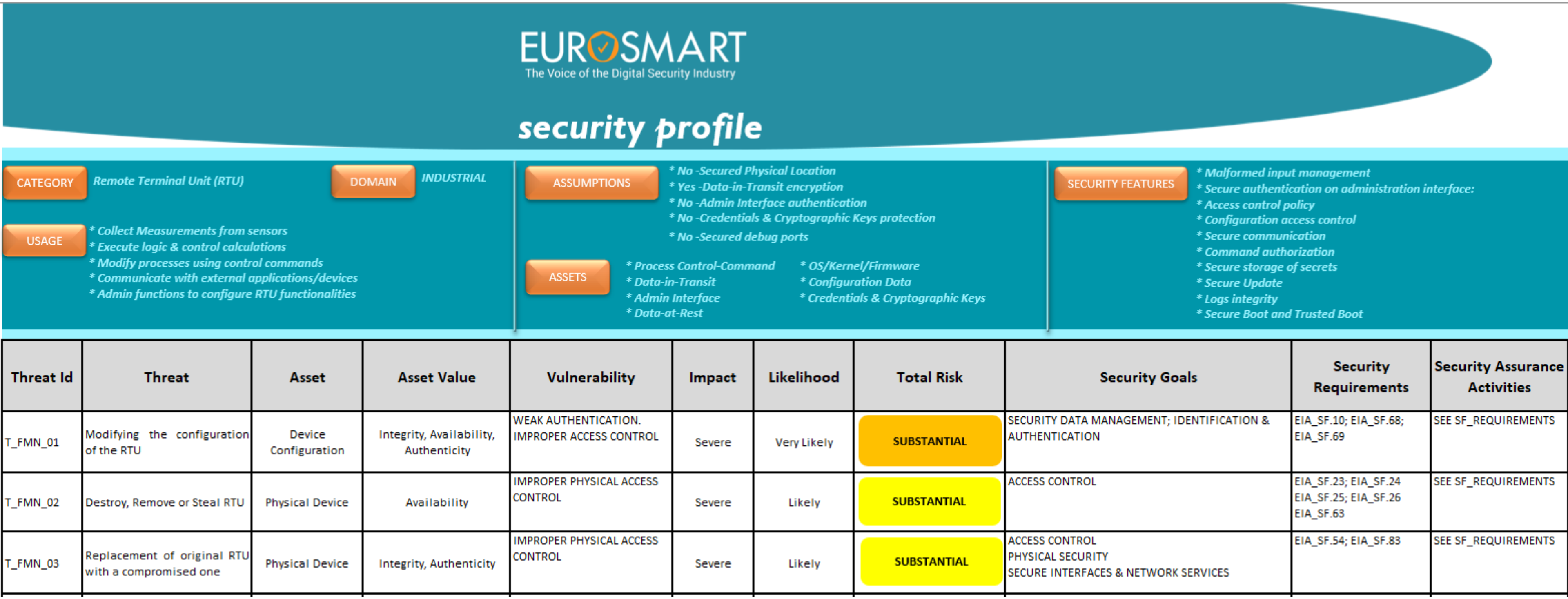
Decide

Risk	Accept	Avoid	Reduce	Transfer
Man in the middle			✓	

Security goal = Confidentiality
Security requirement = Encryption

EUROSMART
The Voice of the Digital Security Industry

A security profile looks like this:



EUROSMART
The Voice of the Digital Security Industry

security profile

CATEGORY: *Remote Terminal Unit (RTU)*

DOMAIN: *INDUSTRIAL*

USAGE:
- ** Collect Measurements from sensors*
- ** Execute logic & control calculations*
- ** Modify processes using control commands*
- ** Communicate with external applications/devices*
- ** Admin functions to configure RTU functionalities*

ASSUMPTIONS:
- ** No -Secured Physical Location*
- ** Yes -Data-in-Transit encryption*
- ** No -Admin Interface authentication*
- ** No -Credentials & Cryptographic Keys protection*
- ** No -Secured debug ports*

ASSETS:
- ** Process Control-Command*
- ** Data-in-Transit*
- ** Admin Interface*
- ** Data-at-Rest*
- ** OS/Kernel/Firmware*
- ** Configuration Data*
- ** Credentials & Cryptographic Keys*

SECURITY FEATURES:
- ** Malformed input management*
- ** Secure authentication on administration interface:*
- ** Access control policy*
- ** Configuration access control*
- ** Secure communication*
- ** Command authorization*
- ** Secure storage of secrets*
- ** Secure Update*
- ** Logs integrity*
- ** Secure Boot and Trusted Boot*

Threat Id	Threat	Asset	Asset Value	Vulnerability	Impact	Likelihood	Total Risk	Security Goals	Security Requirements	Security Assurance Activities
T_FMN_01	Modifying the configuration of the RTU	Device Configuration	Integrity, Availability, Authenticity	WEAK AUTHENTICATION. IMPROPER ACCESS CONTROL	Severe	Very Likely	SUBSTANTIAL	SECURITY DATA MANAGEMENT; IDENTIFICATION & AUTHENTICATION	EIA_SF.10; EIA_SF.68; EIA_SF.69	SEE SF_REQUIREMENTS
T_FMN_02	Destroy, Remove or Steal RTU	Physical Device	Availability	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL	EIA_SF.23; EIA_SF.24 EIA_SF.25; EIA_SF.26 EIA_SF.63	SEE SF_REQUIREMENTS
T_FMN_03	Replacement of original RTU with a compromised one	Physical Device	Integrity, Authenticity	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL PHYSICAL SECURITY SECURE INTERFACES & NETWORK SERVICES	EIA_SF.54; EIA_SF.83	SEE SF_REQUIREMENTS

RISK-BASED - SECURITY ASSURANCE ACTIVITIES

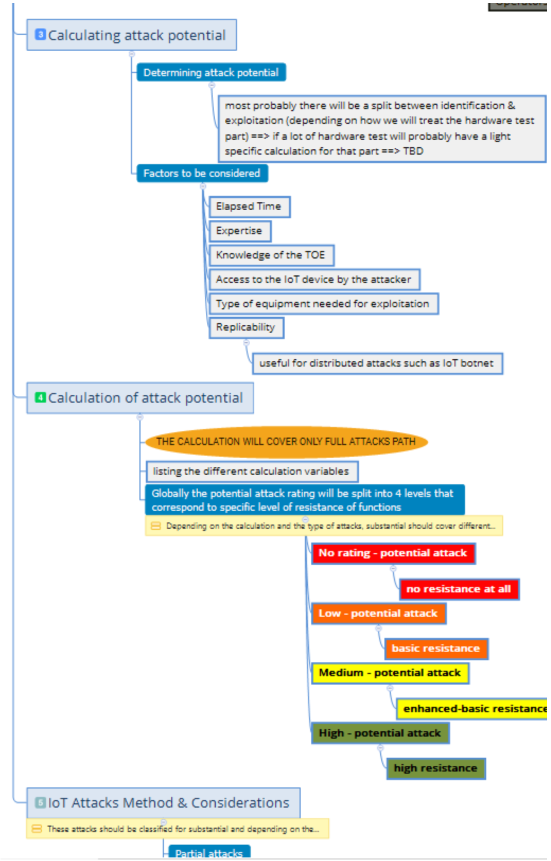
SUBSTANTIAL

IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting
MODERATE (3)				view w yTesting sis (if applicable) ning esting essTesting
MINOR (2)			VA.VulnerabilityScanning VA.BasicRobustnessTesting	view w yTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting
LOW (1)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning

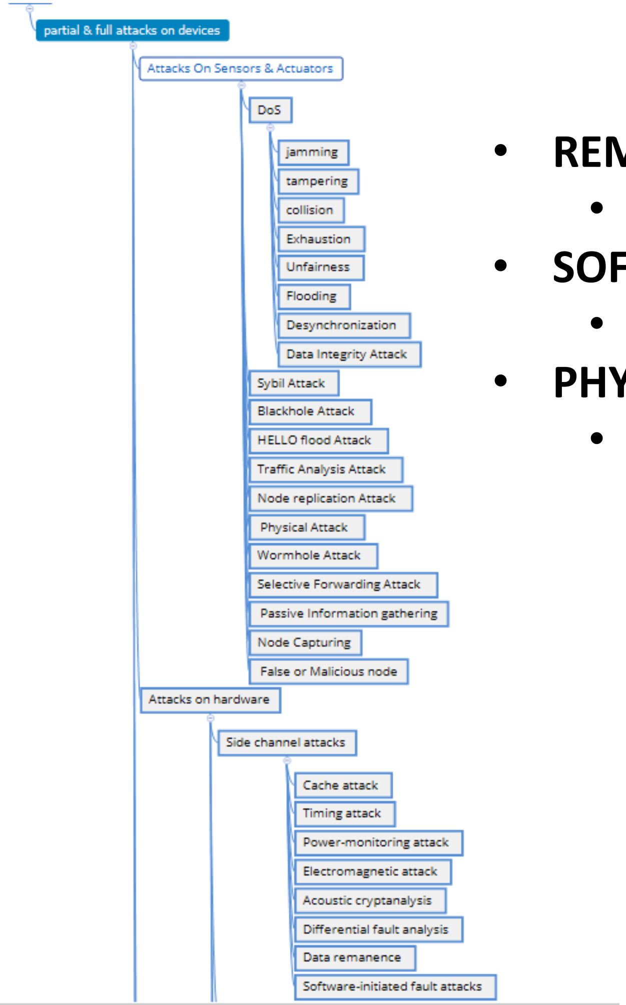
- **Conformity Analysis** (Doc Review, Source Code Review, Composition Analysis, Security Functional Testing)
- **Vulnerability Analysis** (Scanning, Basic Robustness Testing, Advanced Robustness Testing, Non-Intrusive Pentesting)

EUROSMART
The Voice of the Digital Security Industry

Attackers Profiles are methodologically selected for Each Security Profile in a risk-based approach



- 3 Calculating attack potential
  - Determining attack potential
    - most probably there will be a split between identification & exploitation (depending on how we will treat the hardware test part) ==> if a lot of hardware test will probably have a light specific calculation for that part ==> TBD
  - Factors to be considered
    - Elapsed Time
    - Expertise
    - Knowledge of the TOE
    - Access to the IoT device by the attacker
    - Type of equipment needed for exploitation
    - Replicability
      - useful for distributed attacks such as IoT botnet
- 4 Calculation of attack potential
  - THE CALCULATION WILL COVER ONLY FULL ATTACKS PATH
  - listing the different calculation variables
  - Globally the potential attack rating will be split into 4 levels that correspond to specific level of resistance of functions
    - Depending on the calculation and the type of attacks, substantial should cover different...
    - No rating - potential attack
      - no resistance at all
    - Low - potential attack
      - basic resistance
    - Medium - potential attack
      - enhanced-basic resistance
    - High - potential attack
      - high resistance
- 5 IoT Attacks Method & Considerations
  - These attacks should be classified for substantial and depending on the...
  - Partial attacks



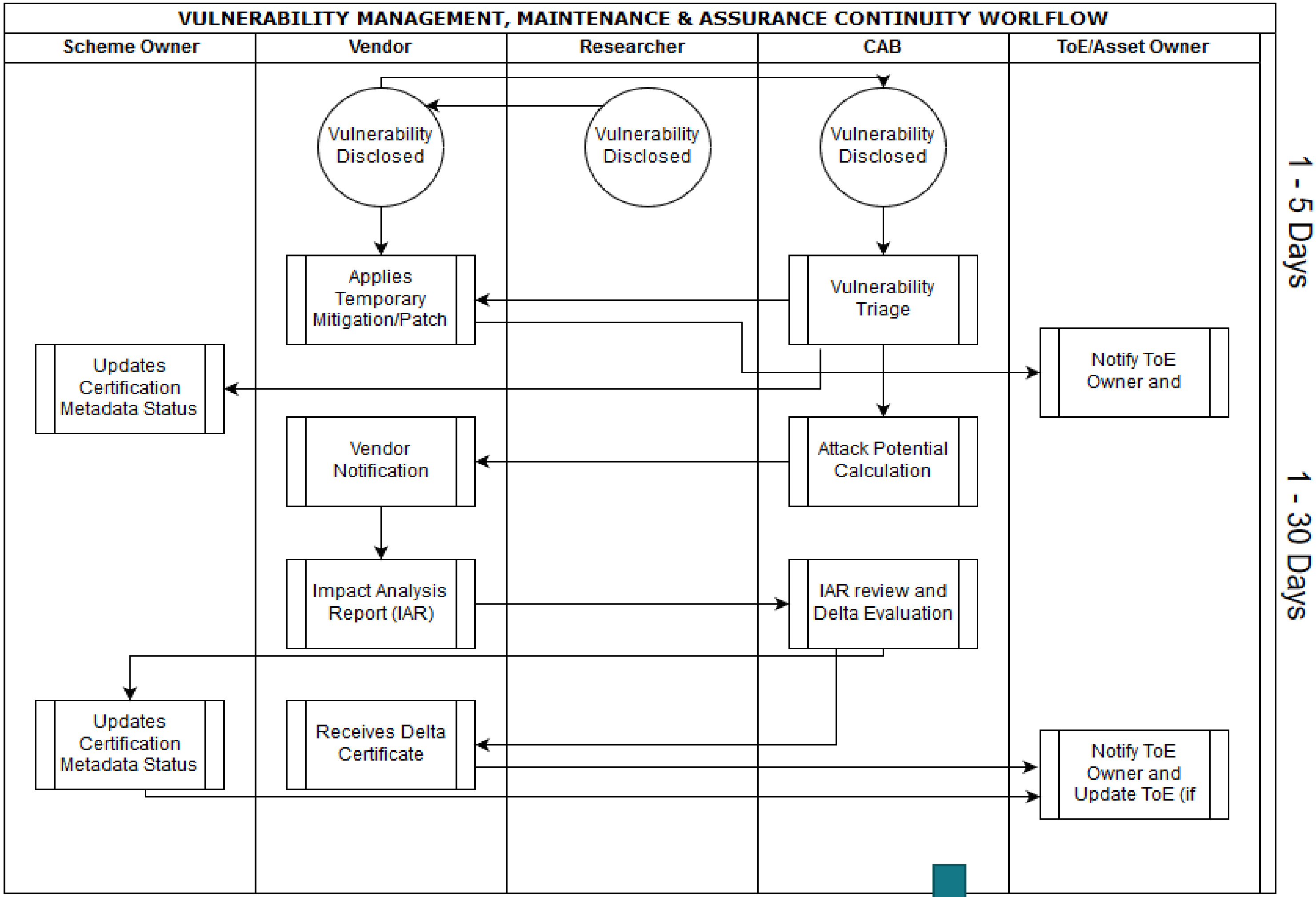
- partial & full attacks on devices
  - Attacks On Sensors & Actuators
    - DoS
      - jamming
      - tampering
      - collision
      - Exhaustion
      - Unfairness
      - Flooding
      - Desynchronization
      - Data Integrity Attack
    - Sybil Attack
    - Blackhole Attack
    - HELLO flood Attack
    - Traffic Analysis Attack
    - Node replication Attack
    - Physical Attack
    - Wormhole Attack
    - Selective Forwarding Attack
    - Passive Information gathering
    - Node Capturing
    - False or Malicious node
  - Attacks on hardware
    - Side channel attacks
      - Cache attack
      - Timing attack
      - Power-monitoring attack
      - Electromagnetic attack
      - Acoustic cryptanalysis
      - Differential fault analysis
      - Data remanence
      - Software-initiated fault attacks

- **REMOTE SCALABLE ATTACKS**
  - (Covered by default)
- **SOFTWARE ATTACKS**
  - (Might be covered)
- **PHYSICAL ATTACKS**
  - (Might be covered)

Temporary Mitigation/Patching

- **Application Layer:**
  - patching with Integration mechanisms are verified once for all by the CAB
- **Core, ROE, HW Layers:**
  - patching first… evaluating later !
    - if and only if the vendor demonstrated a secure maintenance life-cycle process satisfying the flaw remediation requirements.
  - temporary measures will be deployed by the vendor within the time as specified in the Vulnerability Triage Protocol.

Active Monitoring/Vulnerability Surveillance


VULNERABILITY MANAGEMENT, MAINTENANCE & ASSURANCE CONTINUITY WORLFLOW
Scheme Owner
Vendor
Researcher
CAB
ToE/Asset Owner
Vulnerability Disclosed
Vulnerability Disclosed
Vulnerability Disclosed
Applies Temporary Mitigation/Patch
Vulnerability Triage
Updates Certification Metadata Status
Notify ToE Owner and
Vendor Notification
Attack Potential Calculation
Impact Analysis Report (IAR)
IAR review and Delta Evaluation
Updates Certification Metadata Status
Receives Delta Certificate
Notify ToE Owner and Update ToE (if
1 - 5 Days
1 - 30 Days

EUROSMART
The Voice of the Digital Security Industry

[TR-e-IoT-SCS-Part-6]

KEY BENEFITS

01 AUTOMATISATION & AGILE METHODOLOGY

Security Reqs/Questionnaire acts as guidelines, not much overhead evidence docs, and reduced testing time

7-15 m/d w/ security profile

02 RECOGNIZE EXISTING EVALUATION METHODOLOGY

Requirements could be simply mapped to other certification schemes allowing recognition of existing methodologies by composition such as SOGIS CC evaluations for underlying platforms. In any case all types and formats of evidence could be reused as is under this Scheme.

03 REDUCE COSTS

The evaluation addresses priorities and is time-constrained, thus limiting its delays and cost, but still offering a guarantee that experts have spent time analyzing the product most valuable security functionalities

7K$ – 15K$

04 COMPARE IOT DEVICES

The accurate evaluation scope coupled with the security functionalities and the defined set of security requirements are a result of accurate security analysis/threat modelling, The Evaluation metrics and ratings are simple and expressive

05 REQUIREMENTS TAILORED TO THE INTENDED USE

the scope of evaluation focuses on the HW & SW forming the IoT Device but the threat model covers the operational environment including the final application, interfaces and other components connected to the product if any..

KEY BENEFITS

COST-EFFICENT CERTIFICATION MAINTENANCE

06

This Scheme provides a smart framework to define, attest and maintain the certificates delivered for IoT devices after issuance . Patching & Temporary Mitigation are allowed.

CREATE INCENTIVE FOR VENDORS

07

Minimum Effort required on providing evidence, simple metrics, clear requirements, security valued by customer

INVOLVE IOT SERVICE PROVIDERS

08

Expressing SUBSTANTIAL Level Rating + Community creating awareness. IoT Service Providers and Customers trust the vendors

SIMPLE METRICS

09

Requirements and Test Procedures are expressed in simple wording allowing the vendors and CABs to implement and test efficiently.

CYBER SECURITY ACT COMPLIANT

10

This Scheme is a first world-wide to be created while incorporating the Cybersecurity Act principles by design.

CERTIFICATION EXPECTED DURATION

5-12 MAN/DAYS

- **Security Profile Creation**

2-5 MAN/DAYS

- **Vendor Questionnaire Analysis**
- **Installation of the product**
- **Conformity Analysis (docs)**

5-10 MAN/DAYS

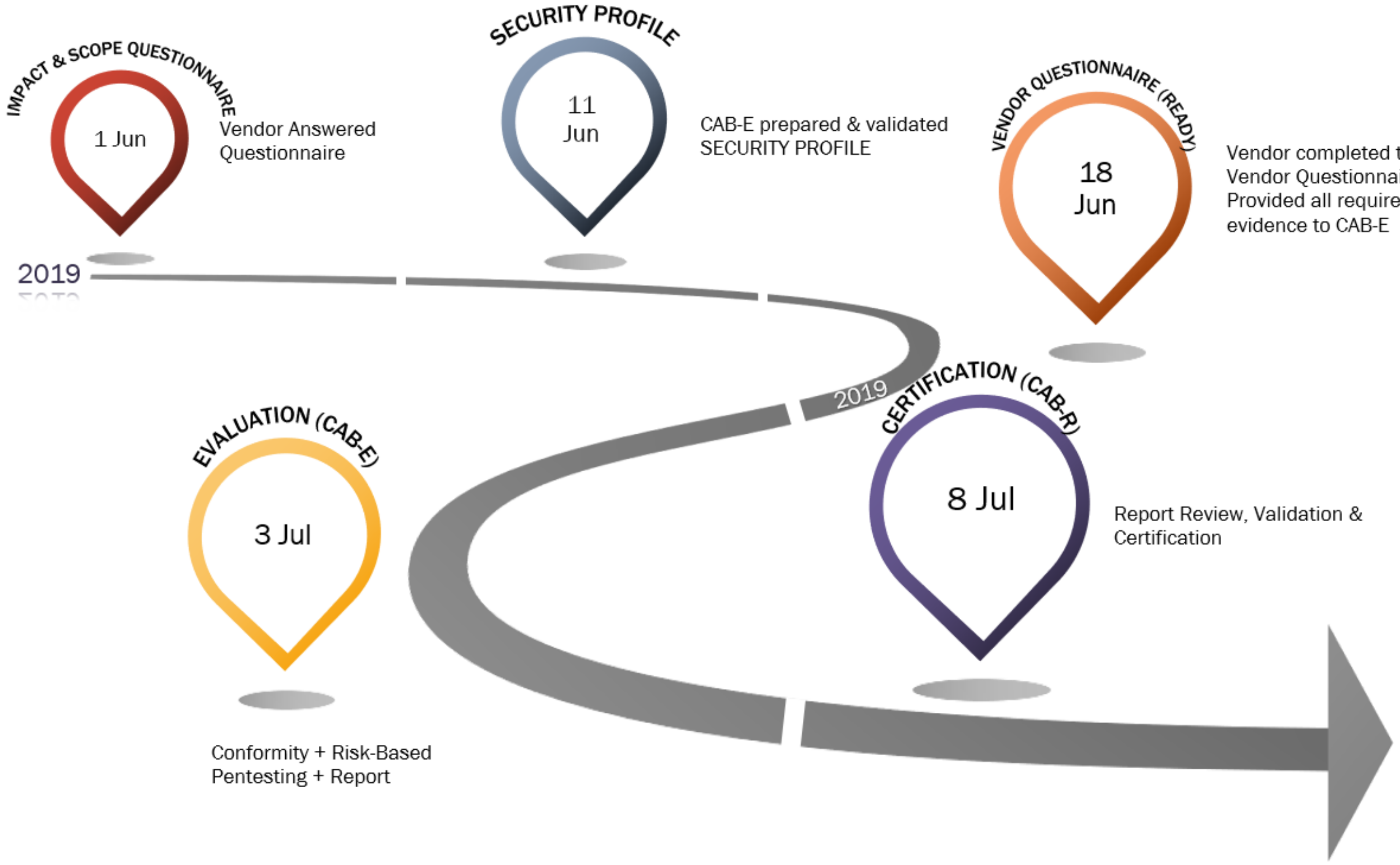
- **Risk-Based Penetration Testing**
- **Evaluation Report Review**
- **Certificate Issuance**

5-12 + 7-15 MAN/DAYS

Pre-defined by the **Security Profile**

EUROSMART
The Voice of the Digital Security Industry

JOIN THE PILOT CERTIFICATION PHASE


2019
IMPACT & SCOPE QUESTIONNAIRE
1 Jun
Vendor Answered Questionnaire
SECURITY PROFILE
11 Jun
CAB-E prepared & validated SECURITY PROFILE
VENDOR QUESTIONNAIRE (READY)
18 Jun
Vendor completed the Vendor Questionnaire & Provided all required evidence to CAB-E
2019
CERTIFICATION (CAB-R)
8 Jul
Report Review, Validation & Certification
EVALUATION (CAB-E)
3 Jul
Conformity + Risk-Based Pentesting + Report

EUROSMART
The Voice of the Digital Security Industry

The END…

In your dreams… Go get Certified first !

THANK YOU

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Eurosmart

Rue de la Science 14b | 1040 Brussels | BELGIUM
☎ Tel. +32 2 880 36 35

ANNEX

EUROSMART

The Voice of the Digital Security Industry

KEY DEFINITIONS

Generic Protection Profile (GPP)

This General Protection Profile (GPP) is a technical report which is based on a generic security risk analysis approach of an IoT Device reference architecture without considering a specific type of data or a context for risk calculation. The main output of this document is a list of security goals and requirements qualifying the need to counter threats identified on a typical IoT device.

[TR-e-IoT-SCS-Part-2]

VENDOR QUESTIONNAIRE

A Vendor Questionnaire (VQ) is a technical document including questions and instructions addressed to the vendor who's implementing the ToE. Responses to these questions are considered as evidence materials and must be provided by the vendor to support the evaluation process.The goal: allow the Vendor to reformulate and refine the security requirements of a Security Profile.

It will draw a list of questions and actions for both the Vendor and the CAB

- VA = actions addressed for the Vendor
- CA = actions addressed for the CAB

[TR-e-IoT-SCS-Part-9]

SECURITY PROFILE

A refinement of the GPP to address specific problem definition of a type of ToE (thermostat, smart cam, etc.) while considering the type and sensitivity of data and the context of the operational environment (e.g. Consumer, Enterprise, Industrial) and the risk factor.

They help to scale security controls and security-related process activities in accordance to the identified risks

A standardized security profile saves a detailed risk analysis for every new product instance.

3 step approach (collect, define and decide)

Risk-based Methodology

[TR-e-IoT-SCS-Part-2]

KEY DEFINITIONS

IoT SERVICE PROVIDER

The IoT Service Provider (IoTSP) could be the IoT device vendor itself or a third-party service provider such as IoT Cloud Platforms (e.g. Azure, AWS IoT, GE Predix, Oracle IoTCS, Google Cloud IoT, IBM Watson IoT, Microsoft Azure IoT Suite, PTC ThingWorx, Kaa Platform, Overkiz IoT Platform, etc.)

METADATA CERTIFICATION STATEMENT

An IoT Metadata Certification Statement (MCST) is a document containing information about a device's characteristics, features and capabilities arranged in a structured manner that can be read and understood by IoT service providers. The reporting format of the metadata statement is generic and therefore can be used to describe any device from any vendor

[TR-e-IoT-SCS-Part-8]

METADATA CERTIFICATION SERVICE

The IoT Metadata Certification Service (MCSE) is a web-based tool where CABs can, on behalf of IoT device vendors, upload signed metadata statements for IoT service providers to access and use as a source of trusted information about a specific device model. Service Providers for IoT Devices will naturally want to be able to trust a device that attempts to make use of their services this makes the deployment of "device metadata service" very useful, secure and scalable in quickly determining if a specific device model is trustworthy to access a resource.

[TR-e-IoT-SCS-Part-8]

EUROSMART
The Voice of the Digital Security Industry

E-IoT-SCS Core Documentation

Reference	Name/Description
[TR-e-IoT-SCS-Part-1]	E-IoT-SCS Process & Policy - This document defines the policies and processes that govern the IoT device certification scheme.
[TR-e-IoT-SCS-Part-2]	E-IoT-SCS Generic Protection Profile + Security Requirements Methodology - This document is a generic representation of common security requirements on IoT devices. It is based on a security risk analysis approach of an IoT Device operating in a typical infrastructure without considering a specific type of data or a context for risk calculation. The main output of this document is a list of security goals and requirements qualifying the need to counter security threats identified on a typical IoT device.
[TR-e-IoT-SCS-Part-3]	E-IoT-SCS Evaluation Methodology - Document defining the evaluation activities to be performed by an evaluator and links between them in order to conduct properly an evaluation. It lists evaluation evidences required to perform actions as defined in the security assurance requirements. It defines way to report evaluation results in Evaluation technical report and observation report. It also provides rules to define verdict and criteria of failure.

E-IoT-SCS Documentation

CABs Accreditation

Reference	Name/Description
[TR-e-IoT-SCS-Part-4]	CABs Agreement - Guidelines listing the rules for setting up agreement between CABs and Certification Scheme stakeholders (e.g. other CABs – CAB reviewer, CAB evaluator, NABs, etc.)
[TR-e-IoT-SCS-Part-5]	CABs Accreditation Policy - Guidelines describing policy for CABs accreditation

Certification Secure Life-Cycle Management

Reference	Name/Description
[TR-e-IoT-SCS-Part-6]	Vulnerability Management, Maintenance & Continuous Assurance Policy: Document describing vulnerability management procedures and the life-cycle management of the Certificate after issuance
[TR-e-IoT-SCS-Part-7]	Mark & Certificate Usage Policy for e-IoT Certification Scheme: Document describing the procedure and conditions which govern the use of the e-IoT SUBSTANTIAL mark and certificate by IoT device vendors, CABs and end-users
[TR-e-IoT-SCS-Part-8]	The Metadata Certification Policy for e-IoT Certification Scheme: Document describing the Metadata Certification Concept and Requirements guaranteeing the relevancy and Authenticity of the Certificates.

Supporting Documents

Reference	Name/Description
[TR-e-IoT-SCS-Part-9]	Templates (Vendor Questionnaire, Impact Analysis Report, Security Profile, Evaluation Report, Mapping Table Concept)
[Informative Annexes]	A set of informative annexes complementing the e-IoT Security Certification Scheme deliverables such as the “e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE”, or “Risk Assessment Methodologies”.

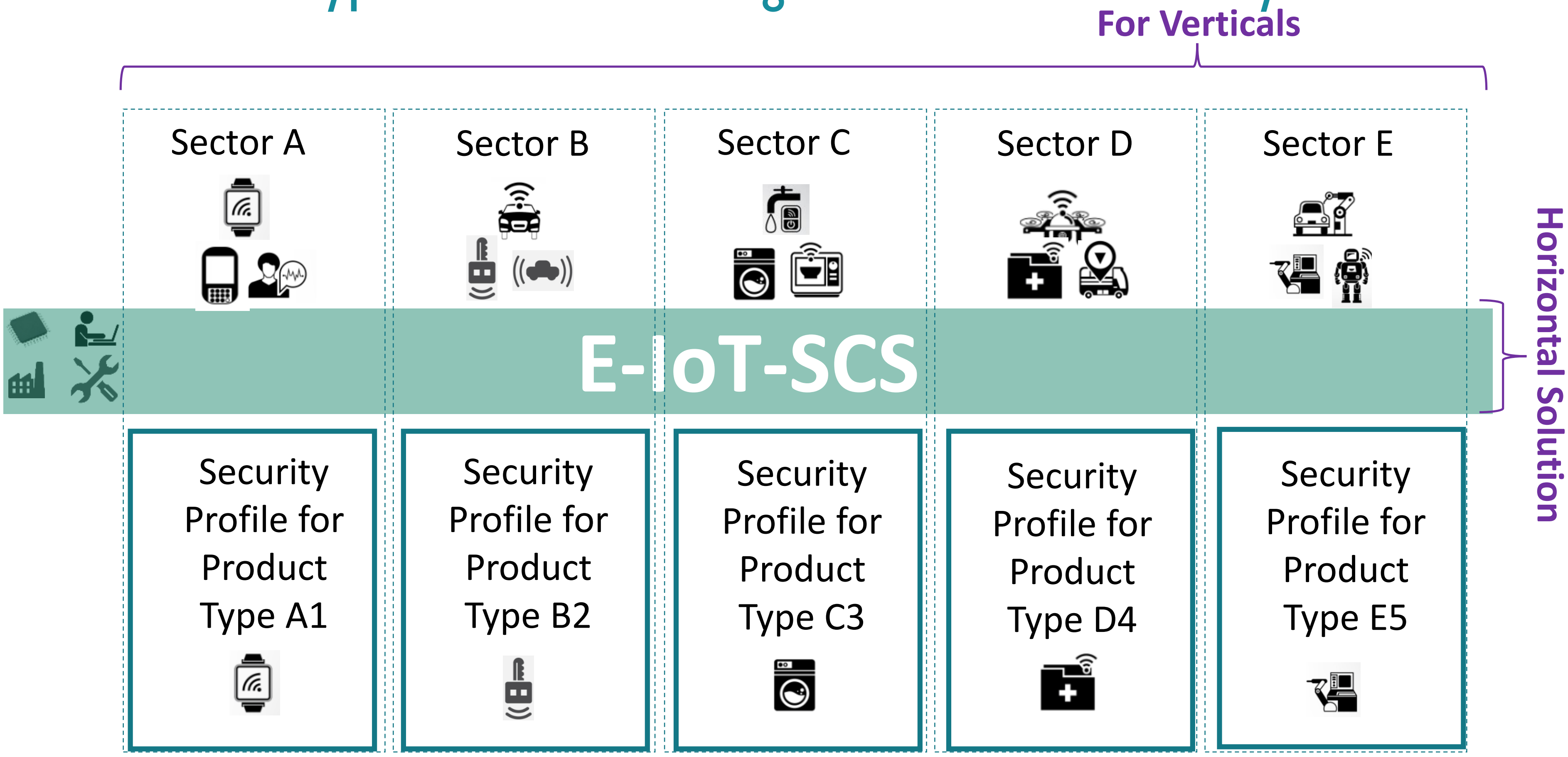
Example of Security Goals

Security Goal (Sample)	Basic	Substantial	High
Strong Authentication		X	X
Firmware Integrity			X
Communication Integrity			X
Strong Encryption		X	X
Data Confidentiality		X	X
IP Protection	X	X	X
Data Availability		X	X
Data Privacy	X	X	X
Human Safety			X

Example of Security Requirements

Requirements (sample)	Basic	Substantial	High
Secure Manufacturer-based Identity & Certificate Storage		X	X
Secure Storage (Tamper Resistant)			X
RNG (FIPS or AIS)		X	X
SHA-256 at least		X	X
Secure Onboarding		X	X
Secure Firmware/SW update (digital signature)		X	X
Secure Event Logging		X	X
Limited Data Collection	X	X	X
End User Data Removal	X	X	X
Secure Cloud-Based Management Services		X	X
Active Product Incident Response Team		X	X
Secure Development Lifecycle (SDLC)			X
Data Privacy (Manufacturing)	X	X	X

IOT Devices may operate in different Operational Environments → each type of IoT device might have several Security Profiles



For Verticals

Sector A

Sector B

Sector C

Sector D

Sector E

E-IoT-SCS

Horizontal Solution

Security Profile for Product Type A1

Security Profile for Product Type B2

Security Profile for Product Type C3

Security Profile for Product Type D4

Security Profile for Product Type E5

Ref. based on ECSO WG1 sources

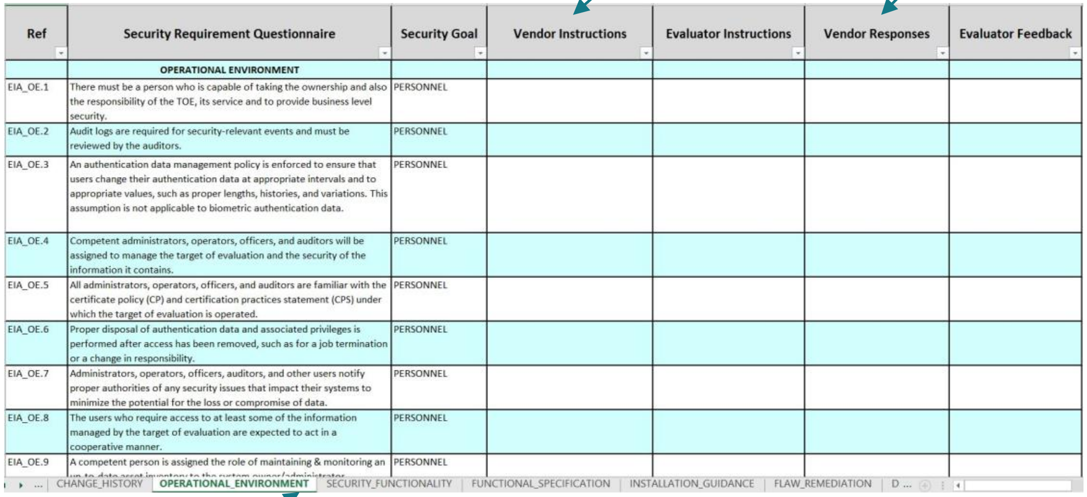
Vendor Questionnaire ?

A Vendor Questionnaire (VQ) is a technical document including questions and instructions addressed to the vendor who's implementing the ToE. Responses to these questions are considered as evidence materials and must be provided by the vendor to support the evaluation process.

Each requirement has an associated instruction which the vendor must follow while providing responses. (explains how to respond)

You will provide your responses inside this column corresponding to each requirement.

VQ looks like this:



Ref	Security Requirement Questionnaire	Security Goal	Vendor Instructions	Evaluator Instructions	Vendor Responses	Evaluator Feedback
	OPERATIONAL ENVIRONMENT					
EIA_OE.1	There must be a person who is capable of taking the ownership and also the responsibility of the TOE, its service and to provide business level security.	PERSONNEL				
EIA_OE.2	Audit logs are required for security-relevant events and must be reviewed by the auditors.	PERSONNEL				
EIA_OE.3	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values, such as proper lengths, histories, and variations. This assumption is not applicable to biometric authentication data.	PERSONNEL				
EIA_OE.4	Competent administrators, operators, officers, and auditors will be assigned to manage the target of evaluation and the security of the information it contains.	PERSONNEL				
EIA_OE.5	All administrators, operators, officers, and auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the target of evaluation is operated.	PERSONNEL				
EIA_OE.6	Proper disposal of authentication data and associated privileges is performed after access has been removed, such as for a job termination or a change in responsibility.	PERSONNEL				
EIA_OE.7	Administrators, operators, officers, auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.	PERSONNEL				
EIA_OE.8	The users who require access to at least some of the information managed by the target of evaluation are expected to act in a cooperative manner.	PERSONNEL				
EIA_OE.9	A competent person is assigned the role of maintaining & monitoring an up-to-date asset inventory to the system owner/administrator	PERSONNEL				

You will find the list of requirements here

Different tabs for each aspect of evaluation. You have to select corresponding tab for providing the responses

The Security Profile contains pointers to all ToE relevant requirements (from the exhaustive list contained in the reference VQ) that must be considered by the Vendor.