



IoT Certification Schemes Cartography

Mohamad Hajj, Claire Loiseaux (Internet of Trust)

Alexander Schasse, Marc Le Guin (TÜVIT)

Last update October 10, 2019

Disclaimer: This document is provided for internal information purposes only. It does not reflect any opinion or position of EUROSMART.
The responsibility of TÜVIT and Internet of Trust is limited to the collection and the aggregation of the answers.

Objectives

- A cartography of 18 schemes applicable to IoT on various criteria
- 18 IoT certification schemes
 - Applicable in Europe
 - Applicable on IoT products/systems
- Various criteria :
 - main targeted product,
 - the associated markets/users,
 - the technical characteristics and
 - the compliance with the European Cybersecurity Certification framework
- Provide a common understanding of the selected schemes based on criteria information

18 Schemes

- **Owned by Public entities**

- **SOG-IS**
- **CSPN (ANSSI)**
- **Baseline certification (BSI)**
- **BSPA (NCSA)**
- **LINCE (CCN)**
- Commercial Product Assurance from CESG (UK)

- **Owned by associations**

- **Eurosmart IoTSCS**
- **GlobalPlatform TEE**
- GlobalPlatform SE
- **IoT Security Foundation**
- **ETSI TS103 655 – Cybersecurity for consumer IoT**
- GSMA IoT Security

- **Owned by companies**

- **ARM PSA L1 and L2**
- **SESIP**
- **UL IoT Security Rating**
- **UL 2900**
- **UL IEC 62443**
- **TÜViT-SQ Security Qualification**

Black (Bold): questionnaire received

Turquoise blue: questionnaire received, scheme website available

Black: questionnaire not yet received

Information Collection Method

1. Questionnaire sent by email to the point of contact communicated by Eurosmart.
2. For some schemes, a first interview is conducted in the aim of clarifying the scope of the study and explaining questions.
3. Reception of a first draft filled by the point of contact.
4. Review of the first draft by IOTR or TÜViT.
5. Interview with the contact point to complete the questionnaire (for some schemes, two interviews were needed to complete the questionnaire).
6. Following the interview, a final version for validation is provided to the point of contact.
7. Finally, the answers are added in the current document for analysis. Note that in case filled questionnaires have been available for the same scheme but from different people, the information provided has been merged.

Report Content

1. Schemes Overview
2. Targeted Market and Users
3. Operational Description and Governance of the Scheme
4. Products Evaluated by the Scheme
5. Evaluation Methodology/-ies used by each Scheme
 1. Evaluation Labs
 2. Evaluation Process
 3. Testing Process
6. Compliance Level with Art.54 of the Cyber Security Act

Scheme Overview

- Age : 80% of the schemes are recent
 - 8 have been launched in 2018 or after
 - 4 have been launched between 2015 and 2018
 - 3 have been launched before 2010
 - 3 No answer provided

- Targeted Markets

Automotive	9
Energy metering	11
Industry 4.0	14
IoT Device (components of PCB)	14
Medical devices	14
Payment applications / online banking	3
Connectivity (eUICC, network products)	7
Government (Qscd, passport, ...)	4
Access control	12
Time stamping	6
General purpose methodology (could be applicable for any markets)	2

Scheme Users

- Almost the same Users for all studied schemes

Chip manufacturers (Silicon and Firmware)
OS Developers
Application Developers
Device Makers
Governments
Service Providers
Product Vendors
End-Customers

Scheme Details

- In the report there is for each scheme the scheme owner, the certificate issuer, the number of issued certificates and certification fees.

Scheme Maintenance, Risk Analysis and Management

- Scheme Maintenance
 - The scheme documentation is managed by a group of identified experts in all schemes
 - The certificate lifetime is either unlimited or limited to 1, 3 or 5 years.
- Risk Management Process
 - 10 schemes support a risk management process during the life cycle of the evaluation
 - 5 schemes support a risk analysis after the certificate issuance
 - 5 schemes do not support a risk management process

Reuse, Composition and Product Level

- Reuse of evaluation and audit results from other schemes
 - 7 schemes allow reuse
 - 3 schemes don't allow reuse
 - 8 No answer provided
- Almost all schemes support composition
- Evaluation Scope
 - 14 schemes Support Component evaluation
 - 8 schemes Support System evaluation
 - 2 schemes Support process/enterprise

Product types

Product Types	Number of schemes
Secure elements (SE)	3
Multi-application processors	7
System on Chip (SoC)	8
xG baseband hardware/software for mobile communication	2
Sigfox baseband hardware/software for IoT services	4
Sensors	8
Hardware Security Modules (HSM)	3
Network devices like routers, switches, etc.	10
Trusted Platform Module (TPM)	4
Security ICs (hardware only)	4
Security ICs including embedded software like operating systems and applications	9
Software applications running on SOC or SE or any mobile environment	10
Software applications running Cloud servers	8
Database servers	8
Qualified Electronic Signature Creation Device (QSCD)	2
General purpose (can be applied for any type of products)	6

Security Evaluation, Support of patching and assurance continuity

- Security Evaluation
 - No security evaluation: 1 scheme
 - Self assessment: 2 schemes
 - Independent evaluation by an approved lab: 12 schemes
 - 14 schemes have already approved labs
 - 1 scheme: Accreditation of labs in progress
- Evaluation level
 - 6 schemes have mono evaluation level
 - 1 scheme has 3 evaluation levels
 - 1 scheme has 4 evaluation levels
 - 3 schemes have 5 evaluation levels
 - 1 has 7 evaluation levels
- Support of patching and assurance continuity
 - 11 schemes support a maintenance procedure and patching

Main Criteria's reflected in the questionnaire

- Testing Process
 - The attack catalog is maintained by a group of expert
 - 5 schemes: no attack catalog available
 - 5 schemes support a black box evaluation
- Evaluation Requirements
 - All schemes require Documentation
 - 9 schemes require the delivery of source code
 - All schemes require Functional Testing
 - 10 schemes require Penetration Testing
 - 4 schemes require Development and Production sites
 - Only one scheme does not have any supporting documents

Compliance with Art. 54 of the Cyber Security Act

- 12 intend to comply to the EU Cyber Security Act
 - 8 claim partial compliance
 - 1 claims full compliance
 - 3 no answer provided

Conclusion

- The work on this analysis resulted in
 - The final report for Eurosmart board,
 - Cross tables relating schemes to Labs and CBs and
 - This slide set.
- The report contains valuable information to see where each scheme stands. Note that the picture will evolve in time. Depending on
 - The market appetite
 - State or EU recommendations
 - ...
- With this report one can easily see what is similar or different in each scheme.



Disclaimer: This document is provided for internal information purposes only. It does not reflect any opinion or position of EUROSMART. The responsibility of TUViT and Internet of Trust is limited to the collection and the aggregation of the answers.



www.eurosmart.com



[@Eurosmart_EU](https://twitter.com/Eurosmart_EU)



[@Eurosmart](https://www.linkedin.com/company/eurosmart)

Thank You

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