EUROSMART
The Voice of the Digital Security Industry

Technical Report

[TR-e-IoT-SCS-Part-1]

Certification Scheme

Process & Policy

Pilot – v1.2

RELEASE

Editor: Roland Atoui – Red Alert Labs

Contributors & Reviewers: François Guerin – Thales, Alban Feraud – Idemia, Rachel Shabat – Winbond, Juergen Noller – Infineon, Sebastian Colle – Infineon, Steffen Heinkel – Infineon, Jonas Andersson – Fingerprint, Eric Vetillard – NXP, Sylvie Wuidart – STM, Jan Eichholz – G&D, Christine Crippa-Martinez – Thales, Franck Sadmi – ANSSI, Jonathan Gimenez - ANSSI

Approved by: Martin Schaffer – SGS, Philippe Proust – Thales, Gisela Meister – G&D, John Boggie – NXP, Stefane Mouille – Cabinet Louis Reynaud

Executive Summary

The European Cybersecurity Certification Framework helps in creating a single cybersecurity market for the EU. A harmonized approach at EU level defines mechanisms that establish EU-wide cybersecurity certification schemes which assess the ICT (Internet and Communications Technology) products, ICT services and ICT processes and make sure they comply with specified security requirements.

The scope of the Eurosmart IoT Security Certification Scheme (e-IoT-SCS) is the Internet of Things (IoT) Device part of a typical IoT infrastructure with a focus on the Basic and Substantial security assurance level as defined by the Cybersecurity Act. At this level of assurance, the certification is intended to minimize the risks of successful attacks on all parts of the IoT infrastructure (device, gateway, connectivity, cloud, application) commonly taking advantage of poor design in IoT devices bringing severe consequences to consumers and vendors, due to non-presence or ineffective security controls. It is indeed vital that IoT devices have security designed-in and verified-in from the outset.

Since these IoT Devices at the low end of the range may have security features constrained by cost, available processing power and performance, size, type of power source, this Certification Scheme considers the trade-off between such constraints, the risks and the cost of certification.

This Certification Scheme introduces 3 new important properties:

1. Security Profile (the "What"):
    - A Security Profile (SP) defines the security functional requirements and security assurance activities specific security problem definition of a type of an IoT Product/Solution (thermostat, smart cam, etc.) while considering the sensitivity of assets, the context of the operational environment and the risk factor. Its definition is a step towards an economic way of dealing with security risk analysis and security targets. It helps to scale security controls and security-related process activities in accordance to the identified risks, i.e. to spend most effort where the highest risks are. This Certification Scheme defines a methodology allowing a harmonized and quick creation of Security Profile covering the full attack surface threat model from Chip to Cloud including the Applications (Business and Mobile), Gateways, the Connectivity and the Cloud.
2. Risk-Based Evaluation (the "How"):
    - The evaluation activities to be undertaken within this Certification Scheme are based on a risk[1] approach and includes a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that IoT Devices implements the necessary security functionalities. Risk-based security evaluation is useful when an ICT product is intended to work in a complex system such as the IoT which requires numerous evaluation activities for adequate coverage in limited time.
3. Certification Validity (the "What if"):
    - Millions of IoT devices are expected to be granted certifications. These certifications must be maintained in a proper and cost-efficient way to guarantee the level of assurance and the certificate in the operational phase. This Certification Scheme defines efficient policies, processes and tools allowing IoT Service Providers, Business Lines, Risk-Owners a Decision Makers to increase their trust in certified IoT Devices.

For a higher level of assurance (level "High" as per the Cybersecurity Act), Eurosmart recommends relying on other relevant Certification Schemes addressing state of the art of attacks.

Finally, within this Certification Scheme, the Cybersecurity Act definitions supersedes over any other definition.

[1] Risk itself is considered a metric that indicates the combination of the consequences of an unwanted incident with respect to an asset and the associated likelihood or estimated frequency of occurrence

	EU CYBERSECURITY ACT - ARTICLE 54	**COVERAGE BY THIS SCHEME**
(a)	subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services	[TR-e-IoT-SCS-Part-1], Chapter 1 + Executive Summary
(b)	a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme.	[TR-e-IoT-SCS-Part-1], Chapter 1 + Executive Summary
(c)	references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II of Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;	[TR-e-IoT-SCS-Part-1], Section 1.3
(d)	where applicable, one or more assurance levels;	[TR-e-IoT-SCS-Part-1], Section 1.1 (BASIC & SUBSTANTIAL LEVEL)
(e)	an indication of whether conformity self-assessment of conformity is permitted under the scheme;	**[TR-e-IoT-SCS-Part-3],** Section 4.2.3 and Section 4.2.10
(f)	where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;	**[TR-e-IoT-SCS-Part-5]**
(g)	The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 51 are achieved;	**[TR-e-IoT-SCS-Part-3]**
(h)	where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;	[TR-e-IoT-SCS-Part-1], Section 4.1 **[TR-e-IoT-SCS-Part-3]** and **[TR-e-IoT-SCS-Part-9]**
(i)	where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;	**[TR-e-IoT-SCS-Part-7]**
(j)	rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;	[TR-e-IoT-SCS-Part-1], Section 4.2 and **[TR-e-IoT-SCS-Part-6]**
(k)	where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;	[TR-e-IoT-SCS-Part-1], Section 6
(l)	rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;	[TR-e-IoT-SCS-Part-1], Section 6.1.4.4.
(m)	rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;	[TR-e-IoT-SCS-Part-1] Section 6.1, 6.1.4 and **[TR-e-IoT-SCS-Part-6]**
(n)	where applicable, rules concerning the retention of records by conformity assessment bodies;	[TR-e-IoT-SCS-Part-1], Section 4.2
(o)	the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;	Refer to "e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE" – [Deliverables Annex], and **[TR-e-IoT-SCS-Part-3]**
(p)	the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;	**[TR-e-IoT-SCS-Part-9]**
(q)	the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;	[TR-e-IoT-SCS-Part-1], Section 5.2
(r)	maximum period of validity of European cybersecurity certificates issued under the scheme;	[TR-e-IoT-SCS-Part-1], Section 6
(s)	disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;	[TR-e-IoT-SCS-Part-1], Section 7
(t)	conditions for the mutual recognition of certification schemes with third countries;	[TR-e-IoT-SCS-Part-1], Section 1.7
(u)	where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;	N/A – Not relevant to the Basic & Substantial level

(v)	format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.	[TR-e-IoT-SCS-Part-1], Section 4.1 **[TR-e-IoT-SCS-Part-3]** and **[TR-e-IoT-SCS-Part-9]**

Date	*Version*	*Description of changes*
15/10/18	V0.1	Initial version created
01/11/18	V0.2	Completed Chapters 6, 10, 11 and 12
05/11/18	V0.3	Minor updates to Chapter 2
16/11/18	V0.4	General updates including EU Cybersecurity Act - Article 47 coverage table
13/12/18	V0.5	Moved the Delta & Derivative Certification to Part 6
22/12/18	V0.6	Re-structuring and general improvements
27/12/18	V0.7	Updated Sections 5 and 6
03/01/19	V0.8	Updated cross-references and hyperlinks
13/02/19	V0.9	Updates considering the latest version of the Cybersecurity Act, specifically Article 47.
05/04/19	V1.0 - Draft	General review and updates (Article 54)
27/05/19	V1.0	BETA - RELEASE
13/09/19	V1.1	Addition of BASIC level and definition + NXP & ANSSI comments
21/10/19	V1.2	PILOT - RELEASE

1 Contents

1 Introduction

This document defines the policies and processes that govern the IoT device certification scheme.

1.1 Scope of the Scheme

This Certification Scheme[2] refines the EU Cybersecurity Certification Framework based on agreement at EU level for the evaluation of the security properties of an Internet of Thing[3] (IoT) device.

The certificate issued will attest that an IoT device has been certified in accordance with such a scheme and that it complies with the specified cybersecurity requirements. The resulting certificate will be recognised in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product.

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 of or services offered by, or accessible via IoT devices throughout their life cycle.

The targeted level of assurance within the meaning of the Cybersecurity Act regulation are **basic** and **substantial**[4].

1.1.1 IoT Definition

For ENISA, IoT is an emerging concept comprising a wide ecosystem of interconnected services and devices, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components. The "Things" collect, exchange and process data to dynamically adapt to a specific context, transforming the business world and the way we live. IoT is tightly bound to cyber-physical system and, in this respect, safety implications are pertinent.

1.1.2 IoT Device Definition

An IoT Device is a "Thing" as per the IoT definition above that is mainly composed of:

- Hardware including microcontrollers, microprocessors, mother board, ICs, physical ports.
- 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

FAQ 1.1

Q1.1: How do I know my product falls into the scope of this scheme?

R1.1: *Please refer to the detailed description of an IoT device and the Target of Evaluation (TOE) described in the Global Protection Profile* **[TR-e-IoT-SCS-Part-2].**

[2] An adopted European Cybersecurity Certification Scheme is a systematic organisation covering Evaluation and Certification of ICT products, ICT services and ICT processes under the authority of ENISA to ensure that high standards of competence and impartiality are maintained, and that consistency is achieved during the whole certification process.

[3] 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.

[4] Note that IoT devices could be certified for a High level of security assurance but this remains out of the scope of this certification scheme

1.2 Disclaimer

EUROSMART and all related entities, provide all materials, work products and, information (“TECHNICAL REPORTS”) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workman like effort, of lack of viruses, and of lack of negligence, all with regard to the TECHNICAL REPORTS, and the provision of or failure to provide support or other services, information, software, and related content through the TECHNICAL REPORTS or otherwise arising out of the use of the TECHNICAL REPORTS.

ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE TECHNICAL REPORTS.

WITHOUT LIMITING THE FOREGOING, EUROSMART DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THESE TECHNICAL REPORTS ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE TECHNICAL REPORTS AVAILABLE, EUROSMART IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS EUROSMART UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE.

ANYONE USING THIS TECHNIAL REPORT SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EUROSMART OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE TECHNICAL REPORTS, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE TECHNICAL REPORTS OR OTHERWISE ARISING OUT OF THE USE OF THE TECHNICAL REPORTS, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THESE TECHNICAL REPORTS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF EUROSMART OR ANY SUPPLIER, AND EVEN IF EUROSMART OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.3 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

1.3.1 General References

Reference	*Name/Description*
[ISO/IEC 17000:2004]	Conformity assessment — Vocabulary and general principles
[ISO/IEC 17065:2012]	Conformity assessment — Requirements for bodies certifying products, processes and services
[ISO/IEC 17067:2013]	Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes

[EU Cybersecurity Act]	European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))
[ISO/IEC 15408]	Common Criteria for Information Technology Security Evaluation (Part 1-3)
[ISO/IEC 18045]	Information technology -- Security techniques -- Methodology for IT security evaluation
[ISO/IEC 17025]	General requirements for the competence of testing and calibration laboratories

1.3.2 Requirements & Evaluation

Reference	*Name/Description*
[TR-e-IoT-SCS-Part-1]	E-IoT-SCS Certification Scheme 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 - 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.

1.3.3 CABs Accreditation

The following documents describe how to become an Accredited CAB

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

1.3.4 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 BASIC and 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.

1.3.5 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".

1.4 Terms and Definitions

Using a common language is very important to formalize the concepts and leverage more objective results. This scheme is based on existing definitions as defined by **[ISO/IEC 17000:2004]**, Common Criteria (ISO 15408), and ECSO Meta-Scheme Approach[5].

Name	**Description**
IoT Device	An IoT Device is an ICT product which is composed of: • Hardware including microcontrollers, microprocessors, mother board, ICs, physical ports. • Software including an embedded OS, its firmware, programs and applications (e.g. OS, Connectivity, Drivers, Bootloader, Cryptographic Libraries, Secure Storage, etc.) • 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
Target of Evaluation	The Target of Evaluation (ToE) defines the scope of the evaluation. It is a set of software, firmware and/or hardware possibly accompanied by guidance documentation. This scheme is addressing the IoT device as a ToE based on a predefined reference architecture.
IoT Product/Solution	An IoT Product/Solution such as a Connected Camera, Smart TV, Smart Thermostat + Mobile Application, a Smart lock, an RTU or a Gateway. It could be composed of one or more IoT devices.

[5] European Cyber Security Certification A Meta-Scheme Approach – December 2017

General Protection Profile	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.
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.
ToE Security Functionality	A ToE Security Functionality (TSF) is combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs
Security Profile	A Security Profile (SP) is a refinement of the GPP to address specific problem definition of a type of an IoT Product/Solution (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. A SP contains a summary of the security requirements that must be covered by the ToE Security Functionality. Its definition is a step towards an economic way of dealing with security evaluation. It helps to scale security controls and security-related process activities in accordance to the identified risks, i.e. to spend most effort where the highest risks are. Security Profiles may be agreed on and standardized for certain product classes. A standardized security profile saves a detailed risk analysis for every new product instance. It provides an accepted standard on security properties of a product.
Security Target	This is where security functionality specific for a given ToE are identified and mapped to the security goals and security functional requirements. In this scheme, a Security Target is based one or several Security Profiles.
Security Goals	The Security Goals are statements of an intent to counter identified threats and/or satisfy identified security policies on the environments and/or assumptions
Security Functional Requirements	Security Functional Requirements (SFR) are the security measures to be implemented by a security functionality and contributes in achieving security goals. This step is valuable specifically when it translates the security goals into a standardised language such as Common Criteria.
Security Assurance & Level	This is the description of how assurance is to be gained that the ToE meets the security goals/requirements. As defined in the Cybersecurity Act, assurance levels provide a corresponding degree of efforts for the evaluation of a TOE and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent cybersecurity incidents. Each assurance level

	should be consistent among the different sectorial domain where certification is applied.
Penetration Testing	During penetration testing, the ToE is tested using various available hacking tools and methods, with the mentality of an attacker. Some of the available tools are collections of specific exploits or attack scripts (real-life attacks), whereas others are commonly used tools for mapping the attack surface or scanning for common weaknesses in software. Penetration tests will use all three testing practices: functional, performance and robustness tests.
Substantial Assurance	Assurance level "SUBSTANTIAL" provides assurance that the ToE meet the respective security requirements including security functionalities and they have been evaluated to a level which aims to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resource. Under this scheme, the evaluation activities to be undertaken depends on each Security Profile and shall include at least the following: 1. a review to demonstrate the absence of publicly known vulnerabilities and 2. penetration testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. The level of effort is pre-defined by each Security Profile.
Basic Assurance	Assurance level "BASIC" provides assurance that the ToE meet the respective security requirements including security functionalities and they have been evaluated to a level which aims to minimise the known basic risks of incidents and cyberattacks carried out by actors with no skills or public resources. Under this scheme, the evaluation activities to be undertaken depends on each Security Profile and shall include the following: 1. a review of technical documentation, 2. a composition analysis when applicable, 3. and when 1 and 2 are not appropriate, substitute evaluation activities with vulnerability scanning. The level of effort is pre-defined by each evaluation.
Operational Environment	Operational Environment where the IoT device is intended to be used. It is essential to set adequate security objectives and subsequently the corresponding security functionalities adequate to the operational environment.
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.)
IoT 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
IoT 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.
Impact Analysis Report	The Impact Analysis Report (IAR) highlights the changes made to a certified product under this scheme. It allows the CAB-R to judge on the nature of impacts due to the change and decide if the vendor requires to fully re-certify, to process only a delta certification or to do no additional actions to amend the certificate.
Security Vulnerability	A security vulnerability is a flaw within the ToE related to software and/or hardware that can cause it to work contrary to its documented design and could be exploited to cause the ToE to violate the security requirements defined in the Security Profile.

1.5 Abbreviations and Notations

Name	***Description***
ToE	Target of Evaluation
GPP	General Protection Profile
SP	Security Policy
ST	Security Target
SG	Security Goal/Objective
SAL	Security Assurance Level
OE	Operational Environment
VQ	Vendor Questionnaire
CAB	Conformity Assessment Body
NCCA	National Cybersecurity Certification Scheme
NAB	National Accreditation Body
ESO	European Standardisation Organisation
CSM	Certification Scheme Manager

TSF	ToE Security Functionality
IOTSP	IoT Service Provider
MCST	IoT Metadata Certification Statement
MCSE	IoT Metadata Certification Service
CAB-R	CAB Reviewer
CAB-E	CAB Evaluator
Q-CAB	Qualified CAB
IAR	Impact Analysis Report
ENISA	European Union Agency for Cybersecurity

1.6 Audience of this document

The primary audience of this Certification Scheme Policy are vendors[6] developing IoT devices (as defined in Section 1.1.2) , CABs undergoing the E-IoT-SCS Certification process and Risk-Owners, Decisions Makers and Business lines involved in an IoT Project.

It is intended to help them understand the process for receiving or issuing certification and the policies applied to this scheme.

1.7 Mutual-Recognition

Until this Scheme is being adopted by ENISA and the European Commission[7], Mutual-Recognition will be granted on a case by case basis according to Security Profiles.

1.8 Instructions

All vendors shall follow the policy outlined in this document to gain Certification for their IoT device implementations.

Reader should follow the step by step process described in Section 4.1 Step by Step Process.

1.9 Support

For help and support, contact e-IoT-SCS@eurosmart.com

1.10 Main Parties Involved

Name	***Description***

[6] A vendor could be an integrator[6] of different components purchased from other vendors.

[7] Once adopted by ENISA and the EC, the resulting certificate of this Scheme will be recognised in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product

Conformity Assessment Body	A Conformity Assessment Body (CAB) that has been accredited by a National Accreditation Body (NAB) (in support of the NCCA) is an organisation, which carries out Evaluations, independently from the developers of the ICT products. A CAB is responsible for carrying out Certification and overseeing the day-to-day operation of an Evaluation.
Qualified CAB	A Qualified Conformity Assessment Body (Q-CAB) is a CAB that is qualified to conduct conformity assessment on the ToE scope as defined in this Scheme.
CAB Evaluator	A CAB Evaluator (CAB-E) performs the evaluation tasks as specified in the Evaluation Methodology **[TR-e-IoT-SCS-Part-3]**: the evaluator receives the evaluation evidence from the vendor on behalf of the sponsor or directly from the sponsor, performs the evaluation sub-activities and completes the Evaluation Report following the template provided in **[TR-e-IoT-SCS-Part-9].** Finally, the CAB-E provides the Evaluation Report to the CAB Reviewer. In case of a basic level evaluation, the CAB-R and CAB-E could perform both evaluation and review.
CAB Reviewer	A CAB Reviewer (CAB-R) reviews the Evaluation Report including the results of the assessment work done by the CAB Evaluator. A CAB-R is responsible for making the certification decision and issuing the Certificate. In case of a basic level evaluation, the CAB-R and CAB-E could perform both evaluation and review.
National Cybersecurity Certification Authority	National Cybersecurity Certification Authority (NCCA) is a representative of a national cybersecurity certification authority. Their main task is to implement and supervise some specific certification schemes covering ICT processes, products and services. Typically, schemes requiring a High level of security assurance. NCCA should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories. Moreover, they should cooperate with other certification supervisory authorities or other public authorities by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes. Takes the role of the CAB in high level of security assurance
National Accreditation Body	A National Accreditation Body (NAB) is responsible of CABs' accreditation in support of the NCCA. NABs are responsible of assessment and continued monitoring of the competence of CABs. NABs shall possess the relevant knowledge, competence and means to properly perform audits to determine if a CAB has the technological knowledge, experience and the ability to carry out assessment
Certification Scheme Owner	A Certification Scheme Owner is carried out by the technical group that created and proposed the Certification Scheme. Its main responsibility is to create, maintain and update the Certification Scheme accordingly. It shall operate within an industrial consortium composed of relevant Certification Scheme Users. In this Scheme, Eurosmart is the Certification Scheme Owner.
Vendor	A company developing the ToE.

	In case of a basic level evaluation, the vendor could perform the vulnerability scanning testing phase and provide the results to CAB-E or CAB-R.
Sponsor	An organization financing the certification of the ToE

These parties get typically involved in the Certification process at the following stages:

1. The Vendor develops an IoT Device.
2. The Sponsor (who can be developer itself) requires a certificate for the developed IoT Device for instance, and hence turns to a Qualified CAB (CAB-E or CAB-R)
3. The CAB-E carries out the Evaluation by assessing the Target of Evaluation (ToE) against security requirements defined by a Security Profile.
4. The CAB-R finally receives and summarises the result of the Evaluation done by the CAB-E and confirms the overall results by issuing the Certificate.

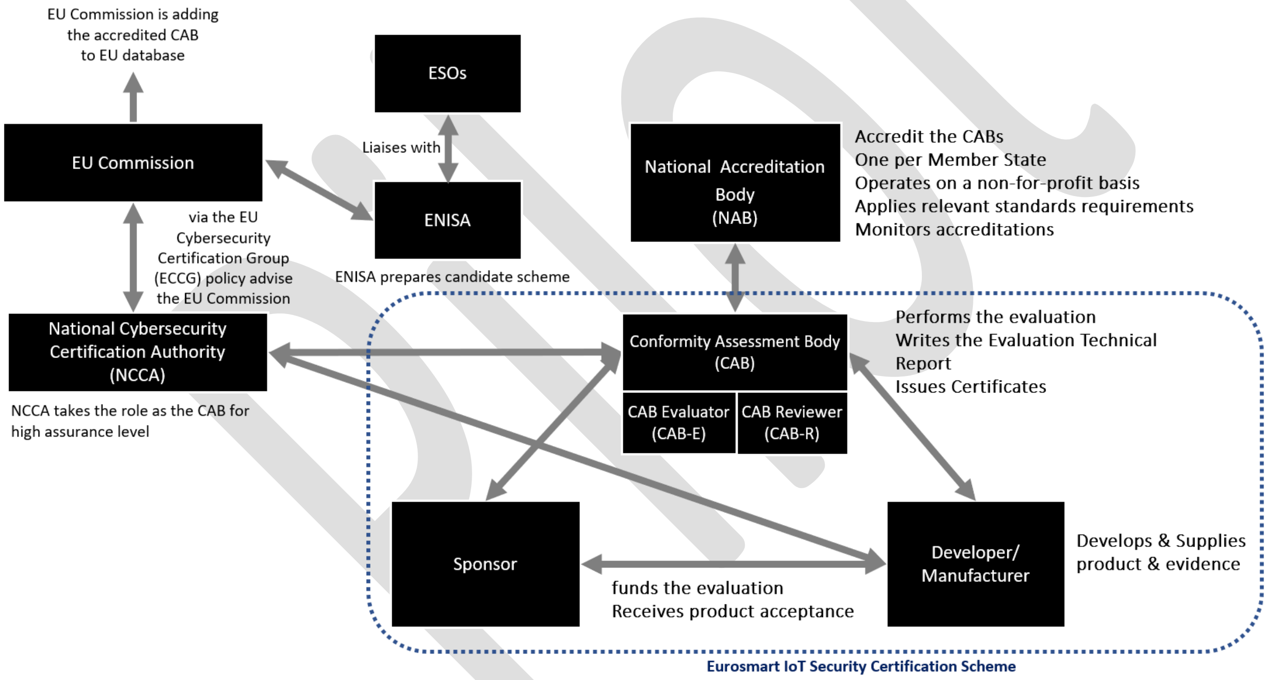

EU Commission is adding the accredited CAB to EU database
ESOs
EU Commission
Liaises with
ENISA
National Accreditation Body (NAB)
Accredit the CABs
One per Member State
Operates on a non-for-profit basis
Applies relevant standards requirements
Monitors accreditations
via the EU Cybersecurity Certification Group (ECCG) policy advise the EU Commission
ENISA prepares candidate scheme
National Cybersecurity Certification Authority (NCCA)
Conformity Assessment Body (CAB)
CAB Evaluator (CAB-E)
CAB Reviewer (CAB-R)
Performs the evaluation
Writes the Evaluation Technical Report
Issues Certificates
NCCA takes the role as the CAB for high assurance level
Sponsor
Developer/ Manufacturer
Develops & Supplies product & evidence
funds the evaluation
Receives product acceptance
Eurosmart IoT Security Certification Scheme

Figure 1: Participants to the EUROSMART Candidate EU Security Certification Scheme

FAQ 1.2:

Q1.2: I am a Developer or a Sponsor, how do I start the certification process?

***R1.2**: Once you have fully prepared your product and all the evidence required for this certification scheme, you should get in touch with one of the CABs (reviewer or evaluator) to initiate a certification process.*

2 Development and Operation of this Scheme

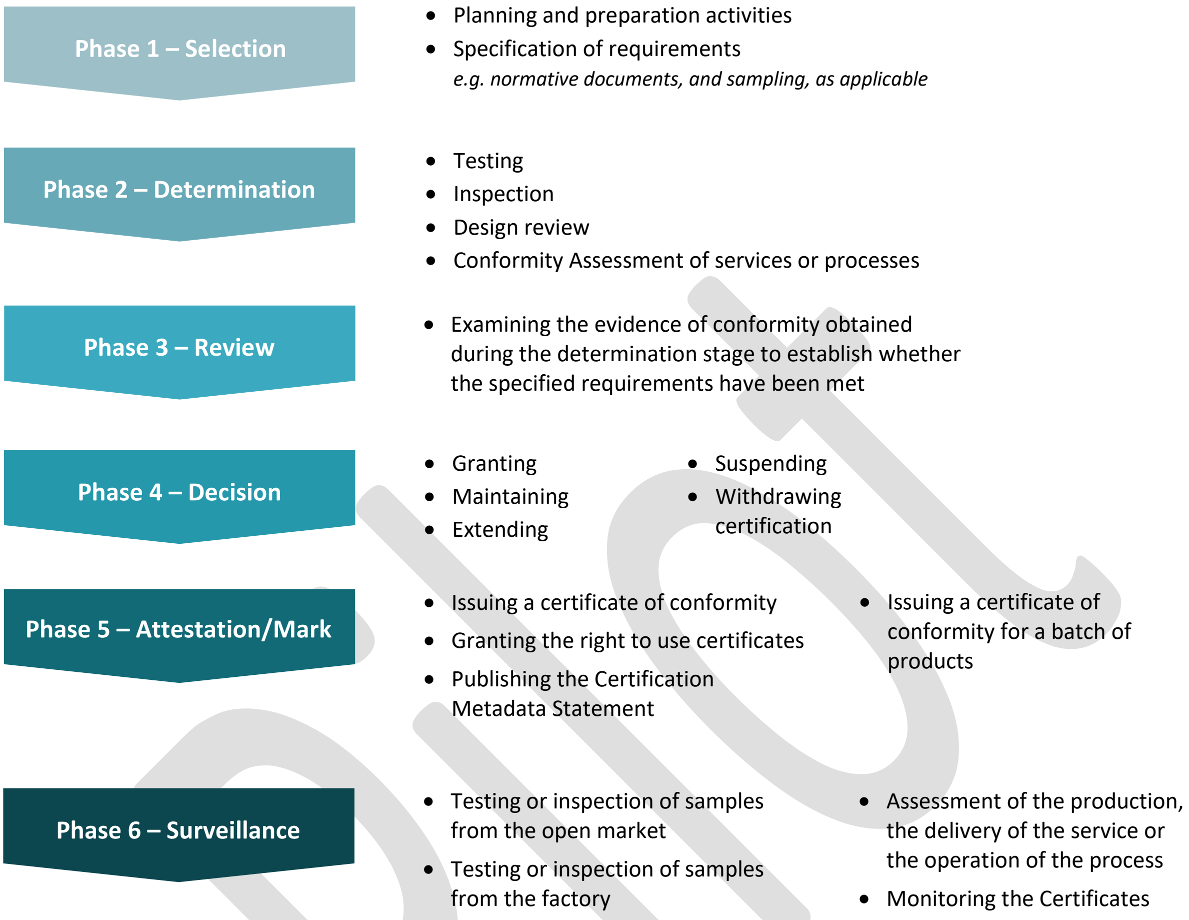
This certification scheme is developed and owned by EUROSMART. As a candidate scheme, it will be operated by the allowed actors defined in the EU Cybersecurity Act regulation once accepted as a European Cybersecurity Certification Scheme.

EUROSMART will be maintaining the scheme on an ongoing basis.

In any case, the Scheme Owner should be responsible of the objectives, the content and the integrity of the scheme and must be able to:

- Maintain the scheme and provide guidance when required.
- Set up a structure for the operation and management of the scheme.
- Document the content of the scheme.
- Ensure that the scheme is developed by persons competent in both technical and conformity assessment aspects.
- Make arrangements to protect the confidentiality of information provided by the parties involved in the scheme.
- Evaluate and manage the risks/liabilities arising from its activities.

3 Certification Process Outline



Phase 1 – Selection

- Planning and preparation activities
- Specification of requirements
  e.g. normative documents, and sampling, as applicable

Phase 2 – Determination

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

Phase 3 – Review

- Examining the evidence of conformity obtained during the determination stage to establish whether the specified requirements have been met

Phase 4 – Decision

- Granting
- Maintaining
- Extending
- Suspending
- Withdrawing certification

Phase 5 – Attestation/Mark

- Issuing a certificate of conformity
- Granting the right to use certificates
- Publishing the Certification Metadata Statement
- Issuing a certificate of conformity for a batch of products

Phase 6 – 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

Figure 2: Certification Process Outline[8]

3.1 Conformity Assessment Results - Acceptance Conditions

This scheme accepts conformity assessment results (including such items as test results and management system certification) which are generated prior to the application or are provided by the vendor. In accordance with **[ISO/IEC 17065:2012]**, 6.2 and 7.4.5, the CAB-R takes responsibility for these conformity assessment results.

In order to cover this responsibility under this scheme, the CAB-R:

- Checks that the conformity assessment results relate to the certification requirements;
- Identifies whether the conformity assessment results come from a body that fulfil the applicable requirements of ISO/IEC 17020 or ISO/IEC 17021 or **[ISO/IEC 17025]**, or are accredited or peer evaluated to these standards with a scope relevant to the certification requirements.

[8] These functions are consistent with the requirements specified in **[ISO/IEC 17065:2012]**, in which the functions selection and determination are together referred to as "evaluation". A description of the functions listed above appears in **[ISO/IEC 17000:2004]**, Annex A

4 Product Certification Scheme

4.1 Step by Step Process

4.1.1 Phase 1 – Selection

Responsible Party	*Process Steps*
Vendor	Develops an IoT Device fitting the scope of this scheme and compliant with the ToE definition as per [TR-e-IoT-SCS-Part-2].
Vendor	If not done before, conduct conformity assessments pre-requisites such as certifying the underlying platform, validate the manufacturing process if required, etc.
Vendor	If a relevant Security Profile (SP) is not publicly available, request from the CAB[9], a SP tailored to his product type, security functionality and operational environment[10]. ***FAQ 1.3*** ***Q1.3: How long it takes to define a SP?*** ***R1.3: An SP requires between 5 to 10 working days of development depending on the IoT device complexity.*** *Please refer to the Global Protection Profile* [TR-e-IoT-SCS-Part-2] *for more details on how to generate Security Profile.*
Vendor	Completes the Vendor Questionnaire (VQ[11]) included in the supporting documents [TR-e-IoT-SCS-Part-9] covering product and processes[12] related security requirements.
Vendor	Fills-in the Application Form that could be found in the supporting documents [TR-e-IoT-SCS-Part-9]. At this stage the CAB-E should have been selected by the Vendor and mentioned in the Application Form. ***FAQ 1.4*** ***Q1.4: How long is my application valid?*** ***R1.4:*** *Your certification needs to be started within the 30 days of submitting your application and the timeline for the assessment is agreed upon convenient dates with you and the CAB.*
Vendor	Selects Qualified CAB-R from the list of accredited CABs.
Vendor & CAB-R	Completes mutual NDAs, signs a Certification agreement, pays necessary fees, signs certification mark agreement, etc.
CAB-R	Reviews the Application for completeness, communicates with the Vendor as needed to clarify any questions.

[9] CABs having a capability of generating SPs must be identified.

[10] If for some reason, the SP cannot be generated by the CAB (e.g. due to an indecision of the risk owner), a SP is generated & delivered using the default risk handling decision (REDUCE) and the certification process is stopped until such a time when the risk owner makes a decision to continue with the process

[11] Note that the generic VQ that is provided in this Scheme is a database covering all possible scenarios. Vendor must answer only a sub-part relevant to their scope as defined in the SP.

[12] Including production and operational processes.

	Approves the Application, when it meets all requirements and make the necessary arrangements with the Vendor for the initial assessment in accordance with the Scheme Evaluation Methodology **[TR-e-IoT-SCS-Part-3].**
Vendor & CAB-E	If required, completes mutual NDAs, signs a Certification agreement, pays necessary fees.

4.1.2 Phase 2 – Determination

Responsible Party	***Process Steps***
Vendor	Sends the VQ, any required evidence documentation and sampling of the IoT device to the CAB-E that was selected and agreed by the CAB-R.
CAB-E	Reviews the VQ, the evidence, and applies the methods specified in the Evaluation Methodology **[TR-e-IoT-SCS-Part-3]** and the procedures specified by this scheme. The goal is to ascertain if the ToE fulfils the security requirements defined in the SP providing a Basic and Substantial level of Security Assurance.[13]
CAB-E	Completes the Evaluation Report following the template provided in **[TR-e-IoT-SCS-Part-9].** This report will be considered as part of the total package of evidence to demonstrate compliance with the certification requirements by the CAB's person or group responsible for making the certification decision.
CAB-E and CAB-R	CAB-E sends the Evaluation Report to CAB-R. ***FAQ 1.5*** ***Q1.5: Is it required that CAB-R reviews the vendor's evidence used to complete the conformity assessment?*** ***R1.5:*** *No, by default, the Evaluation Report must contain enough information allowing the CAB-R to make upon decisions. The Evaluation Report contains only references to the vendor's evidence used during the Determination process to keep records. Upon any doubt, the CAB-R might request to review part of the evidence in order complete to validate a decision.*

4.1.3 Phase 3 – Review

Responsible Party	***Process Steps***
CAB-R	Once all determination activities have been completed, the results of initial product evaluation are reviewed to ensure that they provide a suitable, adequate and effective demonstration that the product and its production and operational environment fulfil the requirements. The review is carried out by a person (or group of people) within a CAB-R who has not been involved in the determination activities. If the evidence is sufficient, a recommendation for certification is made.

4.1.4 Phase 4 – Decision

Responsible Party	***Process Steps***

[13] Note that VQ includes security requirements covering the production and operation phase as well as composite evaluation results

CAB-R	When the outcome of the review is positive, a decision is made to grant certification. When the outcome of the review is negative, a decision is made not to grant certification. The vendor is informed with the reasons for the negative decision. The decision is made by the CAB-R who has not been involved in the evaluation activities. The review and decision may be made by the same person or group of persons working for the same CAB-R.

4.1.5 Phase 5 – Attestation/Mark

Responsible Party	***Process Steps***
CAB-R	Following the decision to grant certification, the CAB-R issues a statement of conformity. Under this scheme, the statement of conformity is in the form of a certificate and a subsequent listing of the certificate on the scheme owner's website by the CAB-R and/or CAB-E, and on the CAB's website. **[TR-e-IoT-SCS-Part-9]** gives an example of information to be included in a certificate of conformity. In addition, the certified vendor may place the scheme's certification mark on the product subject to a licensing agreement being entered with the CAB
Vendor	(if applicable) submits the metadata certification statement to the CAB-R centralized certification server

4.1.6 Phase 6 – Surveillance

Responsible Party	***Process Steps***
CAB	CAB-R and/or CAB-E carry out surveillance as defined in this scheme policy in Section 4.2 to provide confidence that products manufactured after the initial certification continue to fulfil the specified requirements.

4.2 Surveillance

The surveillance activities are selected according to the nature of the product and the consequences and probability of non-conforming products. The frequency with which the activities are carried out is specified in this scheme for each Security Profile and can be adjusted in the light of the results of previous surveillance cycles. For example, if non-conformities in products or the management system have been found, surveillance may be carried out more frequently until the necessary level of confidence is restored.

Surveillance activities cover the manufacturing and the operational phases of the certified product and include one or more of the following:

Activities	***Responsibilities***
a) Inspection of product samples taken either from the point of production, or from the market, or from both for conformity with the certified type;	CAB-R
b) Testing of product samples taken either from the point of production, or from the market, or from both to check that they fulfil the specified requirements;	CAB-E
c) Verification of the validity of the 3rd party compliance certificate covering the production process and auditing of the management system, including examination of the vendor's quality records relating to the production process	CAB-R
d) Active monitoring of latest reported security vulnerabilities impacting the ToE, following the EU CSIRT[14] sources for security alerts.	CAB-R and CAB-E must agree on this activity upon each certification.

Table 1: Surveillance Activities

If surveillance reveals nonconformity with the certification requirements or new vulnerability discovered which cannot be readily remedied by the Vendor, the CAB-R considers what action to take regarding the certificate validity (see Section 6.1).

The Vendor keeps a record of any complaints relating to compliance with the certification requirements and documents the remedial actions taken. The vendor makes the records available to the CAB-R on request. If non-conforming products have been released onto the market, the Vendor informs the CAB-R so that it can agree on the action to be taken.

Finally, the CAB-R shall notify its national CERT about discovered vulnerabilities **[TR-e-IoT-SCS-Part-6]**.

5 Vendors Obligations

5.1 Publicity

The Vendor has the right to publish the fact that:

a) An identified product has been certified;

b) The vendor has been authorized to

- use a valid certificate of conformity, and
- apply a mark of conformity for products to which the licence applies.

In every case, the Vendor takes sufficient care of its publications and advertising so that no confusion arises between certified and non-certified products.

The Vendor does not specify any function or make any claim or the like in user information that could lead purchasers to believe that performance of the product or its use is covered by the certification when in fact it is not.

[14] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

5.2 Records retention

The vendor shall keep and made available a record of the certificate and the technical documentation of all relevant information for a period of twenty years after the date of the certificate issuance.

5.3 Vulnerabilities Management

The vendor must monitor potential new vulnerabilities related to the IoT device which could have impacts on the security functionality of the product and the validity of the Certificate as defined in **[TR-E-IOT-SCS-PART-6].**

In addition, vendors must provide means for contacts allowing researchers or other entities who discovered a new vulnerability to notify them.

6 Certification Validity

Millions of IoT devices are expected to be granted certifications. These certifications must be maintained in a proper and cost-efficient way to guarantee the level of assurance and the certificate in the operational phase.

A granted certificate is considered valid with no sunset date until one of the changes listed below occurs:

6.1 Changes affecting Certification

Certification could be affected for one of the following four changes:

1. Changes to the product requirements
2. Changes to other scheme requirements
3. Changes by the vendors
4. A vulnerability impacting the product was disclosed

The metadata certification concept is intended to provide an attestation for each certified IoT device.

This concept allows IoT service providers, vendors and users to attest the validity of the certificate. IoT Service providers would be able to impose security policies relying on the certification metadata statements provided by the Vendor.

6.1.1 Changes to product requirements

When a standard or another normative document that is part of the certification requirements is changed, there are several factors that must be considered by the scheme owner when he fixes the date on which the new product requirements of the changed document will come into force (effective date reflecting the transition period).

The effective date of obsolescence of a standard or other normative document is communicated by the CAB-R to all applicable Vendors to allow them adequate time to take appropriate action.

In those cases when the standard development organization responsible for the standard or other normative document defines the transition period until which the superseded document is valid, this date defines the obsolescence of the superseded document unless otherwise stated by law or by the scheme.

Further factors that are considered when choosing the effective date include, but are not necessarily restricted to, the following:

a) Compliance with regulations or contractual obligations;

b) The urgency of complying with revised health, safety, or environmental requirements;

c) The length of time and financial costs for retooling and manufacturing a product complying with the revised requirements;

d) The extent of stock on hand and whether it can be reworked to meet the revised requirements;

e) Avoidance of unintentional commercial advantage given to a particular manufacture or design;

f) Operational constraints of the CAB

6.1.2 Changes to other scheme requirements

The scheme owner advises the CAB-R, and their Vendors if necessary, of other changes to the scheme requirements, such as:

- Test and examination procedures where these are not contained in the standards or other normative documents that specify the product requirements;
- Criteria and procedures for acknowledgement or assessment of production processes and audit of management systems;
- Conditions for licensing of the certification mark;
- Qualification criteria and procedures for CABs participating in the scheme

6.1.3 Changes by Vendor

The Vendor's informs the CAB-R about any intended modification to the product, production process or management system which may affect the conformity of the product.

The CAB-R determines whether the announced changes require another initial testing and assessment or other further investigations. In such cases, the Vendor is not permitted to release products under the certificate resulting from such changes until the CAB has notified the Vendor accordingly.

FAQ 1.5

Q1.5: What if my IoT product/solution gets updated multiple times?

R1.5: *In case the ToE is extended to include the IoT application and Mobile application (please refer to the ToE extended definition in the GPP* **[TR-e-IoT-SCS-Part-2])** *and the update is related to the application layer, patching with Integration mechanisms could be verified once by the CAB during the certification process. In that case, vendors are able to securely update the application while preserving the validity of the certificate. In the case where the update is related to the other layers of the ToE (Core, ROE, HW), this scheme allows to patch the ToE first and evaluate later if and only if the vendor demonstrated a secure maintenance life-cycle process satisfying the flaw remediation requirements.*

Since its very common to require a large amount of time to deploy a definitive update/patch for the vulnerability, temporary measures will be deployed by the vendor within the time as specified in the Vulnerability Triage Protocol (see **[TR-e-IoT-SCS-Part-6]***).*

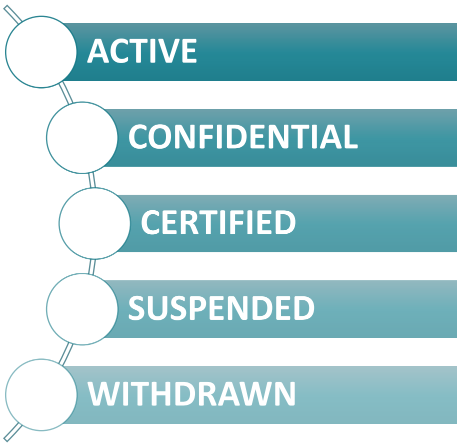
A Vendor wishing to extend the scope of certification to additional types or models of products, to the same specified requirements (same SP) as the products for which a certification is already granted, applies to the CAB using the Impact Analysis Report **[TR-e-IoT-SCS-Part-9].** In such cases, the CAB may decide not to carry out a full re-Certification but a Delta Certification.

If the Vendor wishes to apply the certification to additional types of products, but to different specified requirements (new SP), or if the Vendor wishes to apply for an extension of the certification to cover an additional facility that is not covered by the earlier licence, it will be necessary to perform only those parts of the original application procedure which do not cover the new circumstances.

6.1.4 Certification Status

A list of Certified IoT devices will be maintained by the CAB-R and a public list will be available on their Website.

Certification may be in the following states.



6.1.4.1 Active

Once a certification application is submitted to a CAB-R, the Certification state becomes “Active”. Active applies to initial Certification and Delta Certification.

6.1.4.2 Confidential

Confidential Certification is allowed for companies that wish to complete the Certification process confidentially. Vendors can request their certification remain confidential when applying for Certification.

During a Confidential Certification, only the CAB-R and CAB-E are aware of this procedure. The Certificate will not be announced and will not appear on the CAB’s website until Confidentiality is withdrawn.

Confidentiality may be withdrawn at the request of the Vendor by submitting a written request to the CAB with the corresponding certification number.

6.1.4.3 Certified

A ToE with a “Certified” status is one that has been issued a Certificate and is in good standing.

6.1.4.4 Suspended

The applicability of the Certificate to a specific ToE may be suspended for a limited period, for example in the following cases:

a) If the surveillance shows nonconformity with the requirements of such a nature that immediate withdrawal is not necessary;

b) If a case of improper use of the certificate or the mark (e.g. Misleading publications or advertisement) is not solved by suitable retractions and appropriate corrective actions by the vendor;

c) If there has been any other contravention of the ToT certification scheme or the procedures of the CAB-R.

The Vendor is prohibited from identifying as certified any product that has been manufactured under a suspension of the Certificate as applicable to that product.

A Certificate may also be suspended after mutual agreement between the CAB and the Vendor for a limited period of non-production or for other reasons.

An official suspension of a Certificate is confirmed by the CAB-R in a registered letter to the Vendor (or by equivalent means).

The Vendor may give notice of appeal, and the CAB-R when considering the appeal may or may not (depending on the nature of the case) decide to proceed with its decision to suspend the Certificate.

The CAB-R indicates under which conditions the suspension would be removed, such as for example corrective action taken. At the end of the suspension period, the CAB-R investigates whether the indicated conditions for re-instituting the Certificate have been fulfilled.

On fulfilment of these conditions, the suspension is removed by notifying the Vendor.

6.1.4.5 Withdrawn

A certificate can be withdrawn by the CAB-R. Revocation is an indication that the product is no longer certified and will never return to good standing.

A Certificate is Withdrawn in the following cases:

1. Failure to follow the [TR-e-IoT-SCS-Part-1] (this document), including:
   a. Failure to respond to and address Security Vulnerabilities **[TR-e-IoT-SCS-Part-6]** identified in a Certified ToE.
   b. Failure to report changes made to Certified ToE. To remain Certified after changes, a Vendor must follow the Delta Certification process **[TR-e-IoT-SCS-Part-6],** Section 5
2. If the surveillance shows that the nonconformity is of a serious nature
3. If the Vendor fails to comply with the due settlement of financial obligations;
4. If inadequate measures are taken by the Vendor in the case of suspension
5. Violation of this scheme Trademark & Certification Agreement, if signed.
6. Remained in a “Suspended” state for more than 30 days.

Reasonable attempts must be made by the CAB to contact the Vendor and report the withdrawn event. The Vendor will be given a minimum of 10 days and maximum of 30 days (unless it is a Security Vulnerability, which would be handled as outlined in **[TR-e-IoT-SCS-Part-6]** from first contact to resolve any of the withdrawn events.

If the CAB considers the event to be resolved within the deadline the Certificate will not be withdrawn and will remain in a “Certified” state. If the Vendor submitted Certification Metadata Statements (CMST), the stored version will be updated to reflect the updated certification state.

7 Confidentiality

The CAB is responsible for ensuring that confidentiality of information is maintained by its employees and those of its subcontractors concerning all information obtained as a result of their contacts with the Vendor; this applies also to information obtained at the application stage.

8 Product Liability

In this scheme, all questions related to product liability are dealt within the Product Liability Directive 1985 [15]and other relevant legal system(s).

[15] Product Liability Directive 85/374/EEC is a directive of the Council of the European Union covering liability for defective products.

9 Complaints and Appeals

The Vendor has a right to complain to the CAB about aspects of the service provided. The vendor may also appeal to the CAB against its decisions on issuing, maintaining, extending, suspending and withdrawing certification. In all these cases, the CAB's complaints and appeals process will apply, as described in **[ISO/IEC 17065:2012],** Section 7.13.

10 Relationship to Other Relevant Certification Schemes

Vendors could had gone (or will go) through other certification schemes tailored to parts of the IoT Device. This scheme allows:

10.1 Re-using Evidence & Results

This means that the formalism used is not the focus of this methodology. Vendors would have to make sure that their evidence (documentation, tests, etc.) are oriented by security functionality and not by functional design.

These relationships could be defined with the most common private/public schemes internationally allowing vendors to reduce costs and time on re-certifications (when required).

In addition, this scheme provides a toolbox presented in **[TR-e-IoT-SCS-Part-9]** including a mapping table concept. This mapping table will include the Vendor Questionnaires on the first column, the category of evidence (ADV, ATE, ASE, etc.) it belongs too, the Vendor Proposed evidence/document fulfilling the requirement and a final column for Rationale.

Questionnaire	***Category***	***Provided Evidence***	***Rationale***
The Vendor must provide an explicit description of the TOE logical and Physical boundary.	ASE / Documentation	Security Target Section 2.1 or Security Policy ***Section 1.2*** or .ppt file attached, etc.	Our TOE is an IoT Device which is composed of a software application embedded on PCB with a hard case. Please find more details about the boundary in the provided evidence …***chapter 1.2***.

10.2 Composite Evaluation (e-IoT-SCS or SOG-IS)

In the sense where other certification processes results could be recognized by this Scheme. These latter could be based either on this same certification scheme applied on a part of the ToE for instance (e.g. Secure Element, or an IoT RoE) or on Common Criteria/SOG-IS third-party certification scheme.

As a matter of fact, some vendors could have already gone (or are planning to go) through a Common Criteria scheme to certify their ICT products. This could be for instance a component (e.g. Secure Element, Secure Flash Memory, Biometric Sensor, etc.) that would fit in an IoT device. Supposing it provides, as a standalone component, a higher level of security assurance, the e-IoT-SCS composite evaluation approach recognizes and reuses such certification schemes evidence and results in a smart and cost-efficient way.

10.3 Relation to IoT Cloud Platforms

In order for this scheme to take into account the whole infrastructure surrounding the ToE (or ToEx), Security Profiles consider the threat model on the full attack surface of an IoT solution from Chip to Cloud. Security

Requirements on the Operational Environment are therefore defined. The evaluation methodology verifies only the conformity of the infrastructure to third-party standard schemes. For instance, IoT Cloud Platforms must get certified according to the relevant and latest ENISA Cloud Certification Scheme based on the the “Cloud Certification Schemes Metaframework” (CCSM)[16]

[16] https://www.enisa.europa.eu/news/enisa-news/enisa-cloud-certification-schemes-metaframework

11 About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

12 Our members

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.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **Trust CB**, **WISekey**, **Winbond**), laboratories (**Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Renaud**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com
@Eurosmart_EU
@Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com