EUROSMART

The Voice of the Digital Security Industry

Technical Report

[TR-e-IoT-SCS-Part-3]

Evaluation Methodology

Pilot – v1.2

RELEASE

Editor: Ayman Khalil – 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, Roland Atoui – Red Alert Labs, 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

Date	Version	Description of changes
23/11/18	V0.1	Initial version created
30/11/18	V0.3	Structure and initial content completed
07/01/19	V0.4	Evaluation Input & Output activities
01/02/19	V0.5	Updates related to the SAA
12/02/19	V0.6	Taking into account comments provided in an internal review.
27/03/19	V0.7	Clarified the Composite Evaluation Approach
24/04/2019	V0.8	Taking into account comments provided in an internal review.
22/05/2019	V0.9	Preparation for final delivery
29/05/2019	V1.0	BETA RELEASE
13/08/2019	V1.01	Basic Level Integration Update
03/10/2019	V1.1	Including ANSSI & NXP comments
21/10/2019	V1.2	PILOT RELEASE

Contents

Table of Figures

1 INTRODUCTION

Security Evaluations are performed by CABs in order to provide a certain level of confidence (required by service providers, vendors, buyers or consumers) in that the product implements sufficient countermeasures and that these measures are implemented correctly and satisfy the security requirements. Thus, reducing the risk of leaving potential vulnerabilities that could be exploited by attackers intending to compromise sensitive assets.

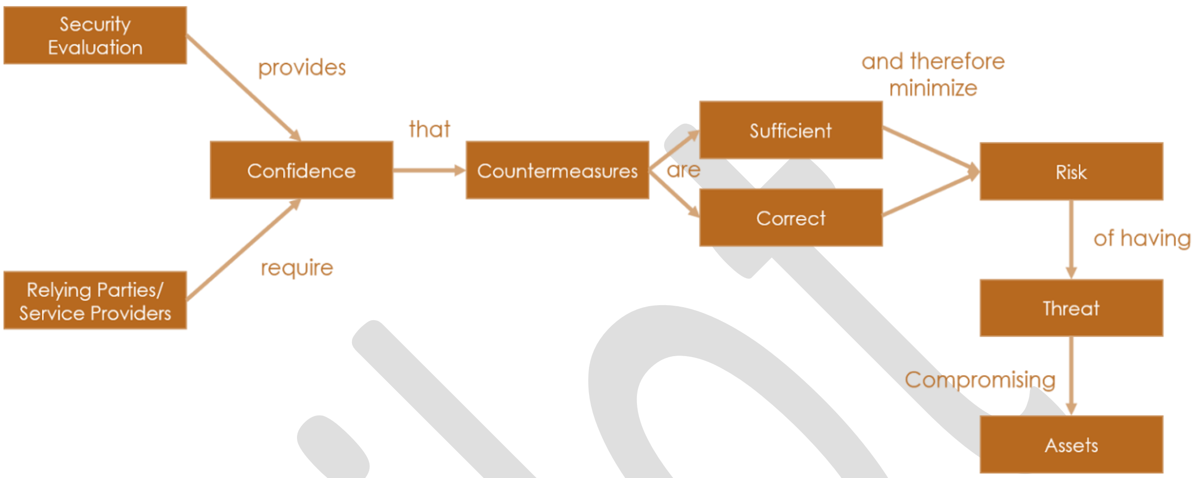

Figure 1: Security Evaluation providing Confidence[1]

In order to achieve greater comparability between evaluation results, evaluations shall be performed within this e-IoT certification scheme as defined in the Process and Policy document [TR-e-IoT-SCS-Part-1].

Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results are submitted to a reviewer independent from the CAB-E who conducted the evaluation.

The CAB-E conducts a detailed review of the product security functionality while performing in parallel the necessary tests to ensure they are working properly; they are effective and presents no major (not contained) vulnerability.

In an Information System, the assurance that "everything will be fine" is important. But to guarantee that, there are several things to check, all the evaluation activities could be done in depth. Therefore, the most common checks, in their different levels of strength, are defined in this document.

The philosophy of this evaluation methodology is to assert that basic and substantial security assurance results from the application of a pre-defined risk-based evaluation effort and the goal is to apply the minimum effort required to provide such security assurance level.

1.1 Risk-Based Security Evaluation Methodology

We presented in the General Protection Profile [TR-e-IoT-SCS-Part-2] a security risk analysis methodology to select the security requirements. The risk assessment comprises the identification of assets, threats and vulnerabilities as well as the identification and propagation of risk treatments (i.e.

[1] Based on Common Criteria definitions and principles

security controls and other counter measures). 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.

A Security Profile includes all these elements in a synthetical representation allowing both the Developer and the CAB-E to act upon the security requirements adequately. It helps to optimize the security by design process and to focus the security evaluation activities onto the most sensitive areas.

Risk-based security evaluation is useful when a product is intended to work in a complex system such as the Internet of Things which requires numerous evaluation activities for adequate coverage in limited time.

It addresses the problem that, although in theory it is indeed desirable that a product is tested as extensively as possible, in practice there are time and budget constraints that make a systematic selection of evaluation activities necessary.

1.2 Risk-Based Security Assurance Model

The Security Assurance Approach provided in this Scheme is the base for demonstrating how the product satisfies a security requirement defined in the Security Profile. If validated during the evaluation process, the CAB delivers the certificate accordingly.

The Security Profile will prioritize various Security Assurance Activities as defined in Section 4, the required evidence for each approach, and the time allocated for the evaluation.

1.3 Composite Assurance Model

This evaluation methodology supports composition in the sense that it could define a relationship to (or recognize) other certification processes results. These latter could be based either on the same certification scheme applied on a part of the ToE for instance (e.g. Secure Element, or an IoT RoE) or on an EU third-party certification scheme[2] (e.g. Common Criteria/SOG-IS, EU Cloud Certification Scheme, etc.).

As a matter of fact, some vendors could have already gone (or are planning to go) through other certification schemes 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 approach is not intended to reinvent the wheel but to allow re-cognizing or reusing such certification schemes evidence and results in a smart and cost-efficient way.

In addition, the formalism used in this Scheme is based on a human natural language and could be therefore easily mapped to other formalisms/languages through mapping tables. This assumes that vendors would have to make sure that their evidence descriptions (documentation, tests, etc.) are oriented by security functionality and not by functional design.

These relationships could be either pre-defined with the most common private/public schemes internationally or could be created on the need allowing vendors to reduce costs and time on re-certifications.

Figure 2 provides a high-level logical layer for IoT devices. On the first hand, the lower we get in the stack the lower the number of products (MCUs, MPUs, SEs) on which high security focus is required

---

[2] This scheme considers composition on top of parts certified according to another EU Cybersecurity Certification Scheme. Indeed, recognition within EU is automatic only for EU cybersecurity certification Schemes, not for non-EU third party schemes **unless** these are formally recognised as equivalent to a given EU Scheme by any EU legislative act.

(more CC like). On the other hand, the higher in the stack the easier it should be for customers to satisfy security goals which simplifies the evaluation and certification work.

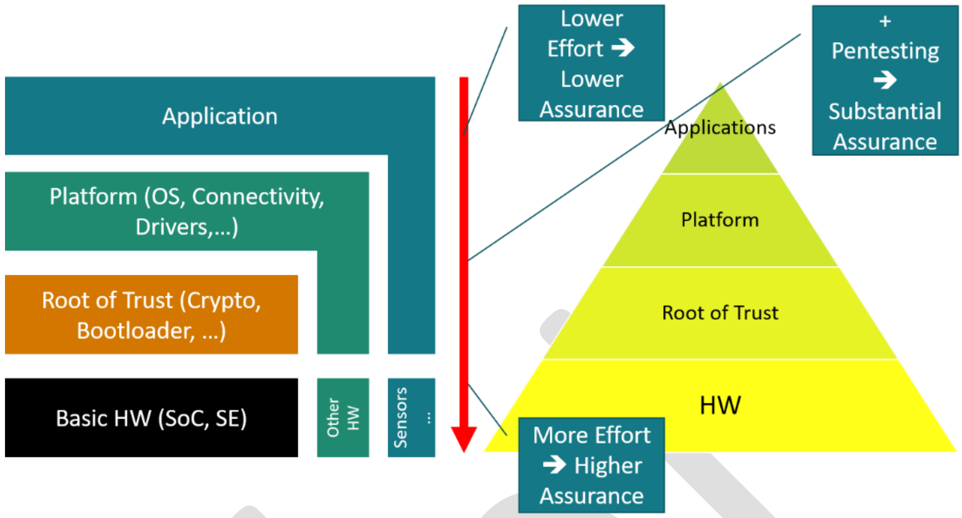

Figure 2: IoT Device Composite Assurance Model

This e-IoT-SCS certification composition concept could cover (but is not restricted to) the following 4 scenarios:

1. IoT Application on a Security Certified[3] IoT ROE[4] (e.g. SE (PPJC), TEE (GPTEE), CSP (PP BSI), TPM, etc.)
2. IoT Application and IoT Core Embedded on a Security Certified IoT Hardware (e.g. IC (PP0084), MCU (CSPN), DSC, CM)[5]
3. IoT Application and IoT Core embedded on an IoT ROE
4. IoT Application and IoT Core embedded on an IoT HW (PCB with multi-purpose Micro-Processor or an MCU Module/SoC)

Note: The choice of certificates that can be used as a basis for composition is limited to those accepted by the CAB-R (in liaison with the NCCA) at the Security Profile definition stage. This limitation is intended to avoid introducing backdoors by which some vendors could obtain a certificate issued according to a scheme not fulfilling the requirements of the targeted level recognized as part of the composite certified product.

[3] E.g. BSI-CC-PP-0084-2014, PP(U)SIM Java Card Platform Protection Profile, CSPN, etc.
[4] Restricted Operating Environment – Refer to [TR-e-IoT-SCS-Part-2] Section 2.3 for a full description
[5] this includes implicitly the IoT ROE considering that a certified IoT HW covers automatically the properties of secure storage, secure crypto, bootloader, etc.)

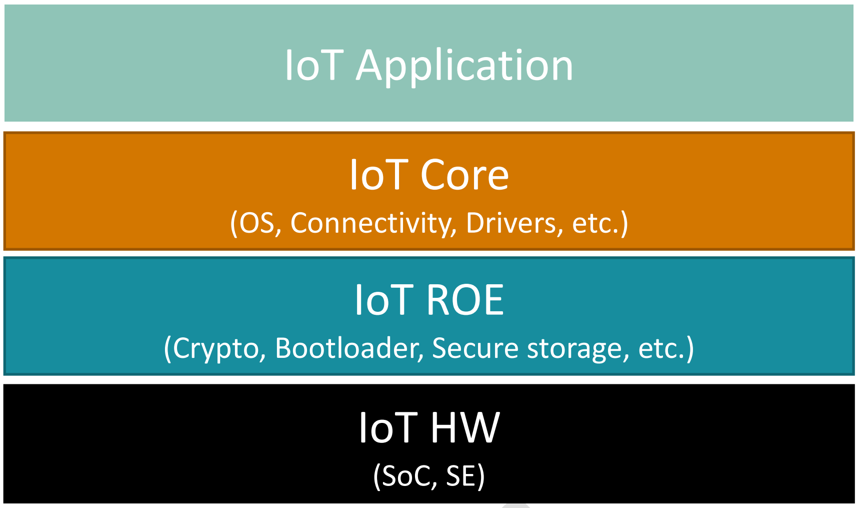

Figure 3: IoT Device in 4 Layers

In order for this composite evaluation methodology to guarantee the same level of security assurance "BASIC" or "SUBSTANTIAL" for all the 4 scenarios, the evaluation effort, time and cost would have to vary accordingly.

This will be tailored to the Security Profile which is applied. For instance, if we take the 1st use case, the evaluation effort is minimal (e.g. if a Secure Element certified under the CC Scheme in compliance with BSI-CC-PP-0084-2014 and is being used in a Smart Lock as a mean for securing the cryptographic keys, the CAB-E won't have to look into the "secure storage" security feature but will focus on the rest of the security features, he might end-up to conduct only 2 days of pentesting on the firmware with a vulnerability scanning on the application side for instance) since the ROE certificate provides already a high level of assurance whereas in the 3rd use case the evaluation requires more effort to provide the targeted level of assurance.

1.4 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.

1.5 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.

1.5.1 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
[ETSI TR 101 583]	ETSI Methods for Testing and Specification (MTS); Security Testing; Basic Terminology V1.1.1 (2015-03)
[ISO-CC]	ISO, "Information technology - Security techniques - Methodology for IT security evaluation", ISO/CEI 18045:2008, 2008.

[CSPN]	First Level Security Certification for Information Technology Product, 2018
[GP TEE]	GlobalPlatform, Device Committee, *"TEE Protection Profile"*, Ref. GPD_SPE_021, Version 1.2.1, November 2016.
[JIL-Smartcard]	*SOGIS*, "Joint Interpretation Library, Application of attack potential to smartcards", *Version 2.9, January 2013.*
[ENISA-Baseline]	Baseline Security Recommendations for IoT in the context of CII - 2017

1.5.2 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.

1.5.3 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

1.5.4 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.

1.5.5 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".

.0

1.6 Abbreviations and Notations

Refer to **[TR-e-IoT-SCS-Part-1]**, Section 1.5

1.1 Audience of this Document

The primary audience of this documents are sponsors, developers and CABS (CABs-E and CAB-R) undergoing the E-IoT-SCS Certification process.

It is intended to help them mainly understanding the global evaluation process as well as apprehending the different inputs and outputs of an evaluation.

1.7 Support

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

2 EVALUATION PROCESS OVERVIEW

2.1 Objectives

This section presents the general model of the methodology and identifies:

- roles and responsibilities of the parties involved in the evaluation process;
- the general evaluation model.

The evaluation process may be preceded by a preparation phase where initial contact is made between the sponsor and the CAB-E. The work that is performed and the involvement of the different roles during this phase may vary. It is typically during this step that the CAB-E performs a feasibility analysis to assess the likelihood of a successful evaluation.

According the [ISO/IEC 18045] the evaluation is the process of assessing the ToE against defined criteria.

These criteria could consist for instance of documentation review, black-box, grey-box or white-box testing. Manual Evaluation can be mixed with Automated Evaluation, for instance fuzzing or penetration testing techniques.

2.2 Roles and Responsibilities

The general model defines the following roles: sponsor, developer, CAB-E and evaluation

authority.

VENDOR	The developer produces the TOE and is responsible for providing the evidence required for the evaluation (e.g. training, design information), on behalf of the sponsor. In case of a basic level evaluation, the developer could perform the vulnerability scanning testing phase and provide the results to CAB-E or CAB-R.
SPONSOR	The sponsor is responsible for requesting and supporting an evaluation. This means that the sponsor establishes the different agreements for the evaluation (e.g. commissioning the evaluation). Moreover, the sponsor is responsible for ensuring that the CAB-E is provided with the evaluation evidence.
EVALUATOR CAB-E[6]	The CAB-E performs the evaluation tasks as specified in the Evaluation Methodology [TR-e-IoT-SCS-Part-3]: the CAB-E receives the evaluation evidence from the developer on behalf of the sponsor or directly from the sponsor, performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority. In case of a basic level evaluation, the CAB-R and CAB-E could perform both evaluation and review.
REVIEWER CAB-R[7]	The Reviewer reviews the work done by the CAB-E and 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. In case of a basic level evaluation, the CAB-R and CAB-E could perform both evaluation and review.

2.3 Relationship of roles

To prevent undue influence from improperly affecting an evaluation, some separation of roles is required. This implies that the roles described above are fulfilled by different entities, except that the roles of developer and sponsor may be satisfied by a single entity.

[6] a CAB-E is typically an [ISO/IEC 17025:2017] accredited lab (or equivalent) laboratory specialised in the field of IT/IoT Security Evaluation. Refer to [TR-e-IoT-SCS-Part-4] for more details.

[7] a CAB-R must comply with the accreditation criteria and requirements for commercial bodies certifying products, processes and services defined in [ISO/IEC 17065:2012]. Refer to [TR-e-IoT-SCS-Part-4] for more details.

2.4 General Evaluation Model

The evaluation process consists of the CAB-E performing the evaluation input task, the evaluation output task and the Security Assurance Activities. Figure 4 provides an overview of the relationship between these tasks and sub-activities.

In case of a basic level evaluation, the CAB-R could perform the evaluation process.

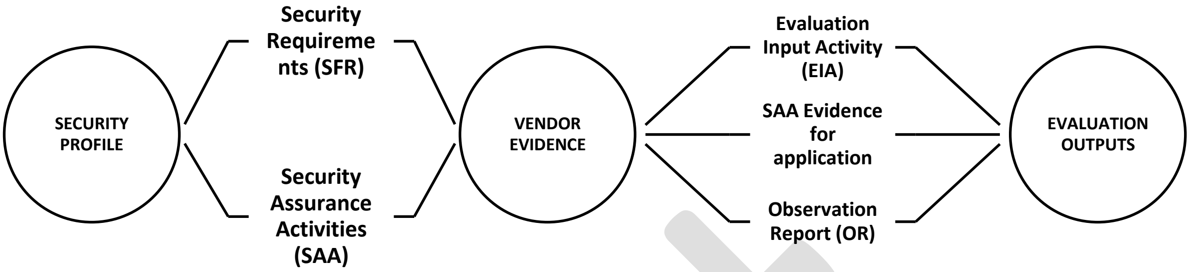

Figure 4: Generic Evaluation Model

The evaluation process may be preceded by a preparation phase where initial contact is made between the sponsor and the CAB-E. The work that is performed and the involvement of the different roles during this phase may vary. It is typically during this step that the CAB-E performs a feasibility analysis to assess the likelihood of a successful evaluation.

2.5 CAB-E Verdicts

This evaluation methodology recognizes three mutually exclusive verdict states: PASS, INCONCLUSIVE and FAIL described below.

2.5.1 PASS

A PASS verdict is granted by the CAB-E after completion of a Security Assurance Activity and determines that the requirement is satisfied.

2.5.2 INCONCLUSIVE

An INCONSLUIVE verdict is granted by the CAB-E after completion of a Security Assurance Activity and determines that the evidence provided by the vendor are incomplete/unclear in order to satisfy the requirement.

2.5.3 FAIL

A FAIL verdict is granted by the CAB-E after completion of a Security Assurance Activity and determines that requirement is not met.

2.5.4 NON-APPLICABLE

A NON-APPLICABLE verdict is granted by the CAB-E after completion of a Security Assurance Activity and determines that requirement is not applicable in the context of the evaluation.

2.6 DRD process

Determination (D), Review (R), Decision (D)

DETERMINATION	Vendor	Sends the VQ, any required evidence documentation and sampling of the IoT device to the CAB.
	CAB Evaluator (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[8].
	CAB Evaluator (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.
REVIEW	CAB Reviewer (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) who has not been involved in the determination activities. If the evidence is sufficient, a recommendation for certification is made.
DECISION	CAB Reviewer (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 client is informed with the reasons for the negative decision. The decision is made by a person (or group of persons) who has not been involved in the evaluation activities. The review and decision may be made by the same person or group of persons.

3 EVALUATION INPUT ACTIVITY

3.1 Roles & Objectives

The developer/vendor is responsible of providing the a completed VQ (Vendor Evidence) including requested evidence to the CAB-E. The objective of this activity is to ensure that the CAB-E has in possession the correct version of the evidence necessary for the evaluation and that it is adequately protected. Otherwise, the technical accuracy of the evaluation cannot be assured, nor can it be assured that the evaluation is being conducted in a way to provide repeatable and reproducible results.

[8] Note that VQ includes requirements on the production phase and composite evaluation results

3.2 Vendor Questionnaire (VQ)

The Vendor Evidence of this activity is a completed version of the Vendor Questionnaire[9].

The Vendor Questionnaire address the following areas when applicable:

3.2.1 ToE Identification

This part defines clearly the IoT device under evaluation, its logical and physical security boundary.

3.2.2 ToE Users

Describes the typical users of the ToE such as:

- Consumers: users with no particular computer and security skills,
- Administrators: users with specific knowledge in the field of use of the product and some security skills
- Security experts: users with proven skills in the field of computer and security

3.2.3 ToE Operational Environment

In this section we will identify relevant assumptions or security organisational policies about the operational environment and how the product will be used. This includes the personnel, physical, organizational, and security procedures and measures required to support the ToE, as well as its dependencies on hardware, software, and/or firmware that is not included within the ToE.

Typically, assumptions or requirements on the mobile application associated with an IoT Device, the gateway or the cloud platform will be part of this section.

Note that this section is essential to confirm the set of security objectives and subsequently the corresponding security requirements and functionality to be addressed during the evaluation.

Self-Assessment of Conformity is permitted for the Operational Environment to confirm the security goals and assumptions.

3.2.4 Security Functionality

In this section, all the security requirements defined in the relevant Security Profile will be mapped to the ToE Security Functionality.

3.2.5 Conformance to Security Profile

This area identifies the claimed conformance to a Security Profile and highlight what is potentially non-conformant with a rationale.

3.2.6 Functional Specification

This area provides the list of logical and physical interfaces allowing access to the security functionality of the ToE.

[9] The VQ will be developed in a generic form to be adapted once for all to all types of ToE. Once combined with a Security Profile (= specific product/type of product) it will provide the exact list of evaluation activities for both the vendor and the CAB.

3.2.7 Installation Guidance

The goal is to describe the platform that will be used to perform the tests on the ToE. This platform must be representative of the typical IoT architecture in which the product is normally used within the limits of the possibilities allocated to the project. The following items are addressed in this area:

- information which enables the installation to be carried out,
- Configuration procedures,
- Scripts necessary to the installation if necessary

3.2.8 Conformance Tests

This could request from the vendor to provide the test cases, tested interfaces and actual results. This is optional but is expected to reduce the time and effort spent by the CAB verifying conformance.

3.2.9 Flaw Remediation

This section ensures that flaws discovered by the ToE consumers will be tracked and corrected while the ToE is supported by the Vendor.

While future compliance with the flaw remediation requirements cannot be determined when a ToE is evaluated, it is possible to evaluate the procedures and policies that a Vendor has in place to track and repair flaws, and to distribute the repairs to consumers.

3.2.10 Development Life-Cycle Process

This section ensures that security by design is addressed by the ToE developers during the whole life-cycle. This covers requirements on the design, manufacturing and development processes to comply security standards.

It is possible to recognize self-assessment or third-party conformity assessment covering procedures and policies that a Vendor has in place at each phase of the life-cycle of the ToE.

3.2.11 Integration

This part addresses the application integration guidance and processes to allow this certification to be valid in the end IoT product incorporating the ToE.

3.2.12 Composition

3.2.12.1 The mapping table concept

A mapping table could be requested in case a vendor reuses existing certification evidence. This mapping table will address the Vendor Questionnaires on the first column, the area 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.

3.3 Management of Evaluation Input

3.3.1.1 CAB-E

The CAB-E shall perform configuration control of the evaluation evidence.

This implies that the CAB-E must be able to identify and locate each item of evaluation evidence after it has been received and is able to determine whether a specific version of a document is in the CAB-E's possession.

The CAB-E shall protect the evaluation evidence from alteration or loss while it is in the CAB-E's possession[10].

3.3.1.2 Scheme Owner

Scheme owner may wish to control the disposal of evaluation evidence (e.g. ETR) at the conclusion of an evaluation.

The disposal of the evaluation evidence should be achieved by one or more of:

- returning the evaluation evidence;
- archiving the evaluation evidence;
- destroying the evaluation evidence.

3.3.1.3 Confidentiality

A CAB may have access to sponsor and developer commercially-sensitive information (e.g.TOE design information, etc.), during an evaluation.

Scheme Owner may wish to impose requirements for the CAB-E to maintain the confidentiality of the evaluation evidence. The sponsor and CAB-E may mutually agree to additional requirements as long as these are consistent with the scheme.

Confidentiality requirements affect many aspects of evaluation work, including the receipt, handling, storage and disposal of evaluation evidence.

4 SECURITY ASSURANCE ACTIVITES (SAA)

The security assurance activities determine according to the impact and the likelihood of a specific identified threat, how the device should be tested against. This approach is based on a list of testing methods such as “Source code review” and “Vulnerability Scanning” that are part of two global activities: Conformity and Vulnerability analysis.

In each section of a testing method, it is identified in the document if it is applicable for basic and/or substantial level. This is done through the field *“Applicability level”*.

[10] This is typically covered by complying to [IEC/ISO 17025:2018] requirements.

Section 4.3 of this document lists the rules that shall be applied in order to list for each security requirement the security assurance activities as described in SECTION 14.3.4.4 of the GENERAL PROTECTION PROFILE [TR-E-IOT-SCS-PART-2] document.

Ref	Security Requirement	Security Goal	Applicable Security Assurance Activity
EIA_SF.1	The device SHALL Use protocols and mechanisms able to represent and manage trust and trust relationships.	DIU INTEGRITY	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting VA.VulnerabilityScanning VA.NonIntrusivePentesting VA.IntrusivePentesting
EIA_SF.2	The device SHALL verify 3rd party software's authenticity and integrity during initialization. If the software authenticity and integrity cannot be ensured, it shall not be installed.	DIU INTEGRITY	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting VA.IntrusivePentesting

Figure 5: Mapping between applicable security assurance requirements and security requirements

4.1 Conformity Analysis (CA)

This activity includes the following three sub-activities:

- CA 1: **Verify** that the ToE claimed [11]security functionality conforms to the security requirements stated in the Security Profile.
- CA 2: **Verify** that all the responses stated in the Vendor Questionnaire are compliant with the ToE handed over to the CAB-E.
- CA 3: **Identify** the requirements that are not applicable [12]in the context of the evaluation.

These three sub-activities could be conducted through the following ways:

4.1.1 Documentation Review

Applicability Level: Substantial and Basic

The CAB-E **reviews** the Vendor's responses provided in the VQ and all related documentation provided to Validate CA 1, CA 2 and CA 3.

Validation Requirements:

The CAB-E shall confirm that the information provided is complete, and the related rationale is consistent with the claims.
The CAB-E shall confirm that the provided information is consistent with each other
Document Review analysis will be tagged CA.DocumentReview in the Security Profile

4.1.2 Source Code Review

Applicability Level: Substantial

The CAB-E **reviews** the Vendor's source code provided in the VQ and all related documentation provided to Validate CA 1 and CA 2.

Validation Requirements:

[11] claimed in the Vendor Questionnaire

[12] "not applicable" means that the device can not answer to the requirement in a demonstrable way. The vendor is not able to select whether a requirement is applicable or not according to the threat model.

The CAB-E shall check manually a sample of the source code accordingly the code review checklist defined by OWASP Code Review Guide [OWASP-RG2]
The CAB-E shall confirm that the developer executed a source code scanning tool (static code analysis) and reports the results to be used during manual code review or during robustness testing.
Source Code Review tests will be tagged <u>CA.SourceCodeReview</u> in the Security Profile

4.1.3 Functional Security Testing[13]

<u>Applicability Level:</u> Substantial

Validation Requirements:

The CAB-E must conduct functional security testing to verify the conformity of the security functionality covering Security Requirements tagged <u>CA.FunctionalSecurityTesting</u> in the Security Profile.
The CAB-E shall complete the Functional Security Testing template provided below for each tested Security Functionality.

The purpose of this activity is to identify the tests to be performed and to describe the scenarios for performing each of the tests, including ordering dependencies to other tests. Further requirements for the test plan (or procedure) may be given in national application notes. It could be an informal description of the tests, but also a description that uses pseudo code, flow diagram, but also concrete reference to e.g. test programs/vectors.

<u>Informative Note:</u>

In contrast with what Functional testing is intended to achieve, which is considering the ToE functionality and functional requirements perspective (It comprises of unit, integration, product, interoperability and conformance testing), Functional Security Testing adopts the same approach but, in addition to benign, legitimate users, Functional Security Testing also considers the possibility of intentional attacks attempting to use the resources from the ToE without legitimate right to use it. Functional Security Testing can address both positive and negative test requirements:

- What the ToE should do, security functionalities such as providing authentication
- What the ToE should not do, security requirements such as not storing confidential data in memory

Functional testing is based on analysing the specification of the functionality of a component or a system without knowledge of the internal structure (black-box testing). Although security tests can be integrated in all phases of testing, the focus is usually in unit and system tests as opposed to integration, conformance or interoperability. Security Functionalities are usually a critical focus area during the evaluation done by CABs.

Many of the details for the Functional Security Testing process can be derived and reused from their definitions given in the conformance test methodology and framework (CTMF) as specified in [ISO/IEC 9646-1]. Most significant difference is that security requirements are often expressed as negative

[13] Functional security testing in the context of this Evaluation Methodology is similar to how it is done in Common Criteria (CC) [ISO/IEC 15408] but using different terminology. It focuses on the Target of Evaluation (ToE) and its Security Functional Interfaces (TSFI) that have been identified as enforcing or supporting Security Functional Requirements (SFRs) identified and stated for the ToE

requirements such as “system should not accept wrong password”, and therefore a certain test objective or requirement can require tens or sometimes millions of unique tests to validate the functionality. When test requirements are mostly negative requirements, the testing approach is called negative testing.

Finally, the process of observations and evaluation regarding test outcome or expected results, can be very different from traditional functional testing as they might require extensive instrumentation of the target system or monitoring of the communications.

4.1.4 Composition Analysis

Applicability Level: Substantial and Basic

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.

Validation Requirements

The CAB-E verifies that the conformity assessment results relate to the claimed scope and certification requirements
The CAB-E 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.
The Composition Analysis tests will be tagged CA.CompositionAnalysis in the Security Profile

4.2 Vulnerability Analysis (VA)

The purpose of the vulnerability analysis activity is to determine the exploitability of flaws or weaknesses in the ToE in the operational environment. In other words, the goal is to determine whether potential vulnerabilities identified could allow attackers to violate the Security Requirements defined in the Security Profile.

This determination is based upon. analysis of the vendor evidence and a search of publicly available material by the CAB-E and is supported by CAB-E penetration testing as described in the application note below p.22.

Validation Requirements

The CAB-E must examine the ToE’s suitability for testing
The CAB-E must identify (public printed sources like books, research papers, CERTs, + focused search in the Vendor’s provided evidence in response to the VQ) and record potential vulnerabilities available publicly
The CAB-E must formulate, produce and conduct basic and advanced robustness testing being focused on Security Requirements that are tagged VA.BasicRobustnessTesting and VA.AdvancedRobustnessTesting in the Security Profile.
The CAB-E must formulate, produce and conduct vulnerability scanning being focused on Security Requirements that are tagged VA.VulnerabilityScanning in the Security Profile.
The CAB-E must formulate, produce and conduct non-intrusive penetration testing being focused on Security Requirements that are tagged VA.NonIntrusivePenTesting in the Security Profile.

The CAB-E must formulate, produce and conduct <u>intrusive penetration testing</u> being focused on Security Requirements that are tagged <u>VA.IntrusivePenTesting</u> in the Security Profile.
The CAB-E must record and examine the penetration testing results in order to decide whether the ToE is resistant to an attacker possessing a SUBSTANTIAL Attack Potential
The CAB-E must not exceed 15 man-days to be spent on all the above listed activities (Unless it is agreed with the vendor)

Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in ANNEX 1.

Application Note
The **SUBSTANTIAL** Attack Potential could be similar to an enhanced-basic attack potential as defined by the CC evaluation methodology. This part will be defined during the Pilot project phase.

The CAB-E **is not expected** to test for attack scenarios beyond those, which possess an Enhanced-Basic attack potential. In some cases, however, it will be necessary to carry out a test before the attack potential related can be determined. Where, as a result of evaluation expertise, the CAB-E discovers a potential vulnerability that is beyond **SUBSTANTIAL** attack potential, this is reported in the ETR ass a **<u>residual vulnerability</u>**.

Application Note
Penetration Testing In 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 above testing practices: functional tests, performance and robustness. First part of a penetration test is to identify the attack surface. This can be done externally or internally. An internal study will look, for instance, at which processes are listening to which network port. A port scanner is a piece of software that will send probes to all network ports in order to trigger responses, mapping the attack vectors by identifying open network services.

4.2.1.1.1 Vulnerability Scanning

<u>Applicability Level:</u> Substantial and Basic

Known vulnerabilities are scanned by trying to trigger vulnerabilities with known attacks, or by checking version information of software from the responses. A vulnerability scanner is a tool that contains a library of vulnerability fingerprints and friendly attacks in order to reveal known vulnerabilities in the system.

4.2.1.2 Robustness Testing (Fuzzing)

<u>Applicability Level:</u> Substantial

Identification of zero-day vulnerabilities is done with fuzzing or static analysis of the code (during source code review). Fuzzing tools, fuzzers, or robustness testing tools send a multitude of generated unexpected and abnormal inputs to a service in order to reveal both known and unknown vulnerabilities.

Robustness testing aims to test that the ToE can tolerate certain level of attacks, and function correctly after the attack. Often referred to as "Fuzzing", this is a form of testing where the ToE inputs are randomly mutated or systematically modified in order to find security-related failures such as crashes, busy-loops or memory leaks. Attackers use these flaws as stepping-stones in order to inject malicious code into the ToE and compromising the integrity of the ToE.

Fuzzing expected to test a live executable IoT Device to uncover unknown vulnerabilities. It is not a conformance activity although it can be used as part of testing the error handling conformity. There is no expected response to a test input, and therefore conformance oracles are very difficult to build for fuzz testing. Fuzzing is typically performed as functional black-box testing through the external interfaces such as networked message sequences, file inputs or user inputs.

This part is split into 2 categories in order to be able to manage better the resource to put in place for the evaluation:

4.2.1.2.1 Basic Robustness Testing

Applicability Level: *Substantial*

Using existing fuzzing templates for known protocol or software.

4.2.1.2.2 Advanced Robustness Testing

Applicability Level: *Substantial*

Necessity of developing specific template for specific protocol or software.

4.2.1.3 Non-Intrusive Penetrating Testing

Applicability Level: *Substantial*

Non-intrusive penetration tests will base its test results on non-hostile checks such as behavioural changes or version information.

Catching a weakness in software requires, for instance, monitoring of network data, logs and events, or process status. Monitoring tools and instrumentation tools, or instruments, analyse the network traffic, the executable binary, operating environment or the operating platform, in order to detect failures and abnormal behaviour that could indicate existence of a vulnerability.

Passive attacks through Side-Channel Analysis using cheap equipment could be part of this activity (e.g. Vertical analysis, Horizontal analysis, Timing analysis.)

4.2.1.4 Intrusive Penetration Testing

Applicability Level: *Substantial*

This is when a penetration test will actually trigger the flaw, often resulting in a crash or system compromise through use of harmless malware. It could conduct by trying out a wide range of hostile attack patterns. Exploit frameworks, or exploitation frameworks are collections of operational malware scripts and tools that will compromise the ToE.

Perturbation attacks based on fault injection using relatively cheap equipment could be part of this activity (e.g. Clock Glitch, Power Glitch) if the attack scenario falls into the substantial level of assurance.

4.3 Rules Applied to Security Assurance Activities Selection for Substantial Level

These rules are applied based on the defined "Base-SAA list" that is described in SECTION 14.3.4.4 of the **GENERAL PROTECTION PROFILE [TR-e-IoT-SCS-PART-2]** document in order to fill the "Final-SAA list".

The rules column precise:

- **Mandatory**[14] (if applicable)**:** means that this test should be automatically listed in the "Final-SAA list" of the Security Profile to be tested by CAB-E **only if it** is listed in the "Base-SAA list",
- **Subject for decision by CAB-E**: for testing methods that should be decided by CAB-E according to specific rules in order to be listed in the "Final-SAA list".

4.3.1 Rules applied to Basic Level

Global Testing Category	Testing Method	Rules to be applied
Conformity Analysis	Documentation Review	Mandatory
Conformity Analysis	Composition Analysis	Mandatory
Vulnerability Analysis	Vulnerability Scanning	Mandatory

4.3.2 Rules applied to Substantial Level

Global Testing Category	Testing Method	Rules to be applied
Conformity Analysis	Documentation Review	Mandatory
Conformity Analysis	Source Code Review	Subject for decision by CAB-E: • If source code exists, it shall be listed in the "Final-SAA list" • If not, Functional Testing Review shall be listed in the "Final-SAA list" instead
Conformity Analysis	Functional Testing Review	Subject for decision by CAB-E: • If source code exists, it shall be listed in the "Final-SAA list" • If not, Functional Testing Review shall be listed in the "Final-SAA list" instead
Conformity Analysis	Composition Analysis	Mandatory
Vulnerability Analysis	Vulnerability Scanning	Mandatory
Vulnerability Analysis	Basic Robustness Testing	Mandatory
Vulnerability Analysis	Advanced Robustness Testing	Subject for decision by CAB-E: • This test shall be listed in the "Final-SAA list" in case of the necessity of developing specific template for specific protocol or software.

[14] "Mandatory" does **NOT** meant that this scheme requires pentesting for each evaluation for instance. Depending on the security profile and the type of product, we expect that pentesting would be required to minimize the **risks of successful cyberattacks at scale** in some cases.

Vulnerability Analysis	Non-Intrusive Penetration Testing	Mandatory
Vulnerability Analysis	Intrusive Penetration Testing	Mandatory

5 APPLICATION OF ATTACK POTENTIAL

Applicability level: only for substantial.

Attack potential is a function of expertise, resources and motivation. This section provides a preliminary method to calculate the attack potential required by an attacker to defeat an IoT Device/Product globally. This latter needs to be tested during the evaluation pilot phase in order to validate the global approach and the final content of the methodology.

The attack potential described in this section is intended to be applied on full attacks. These full attacks are composed of several steps called threats or partial attacks and that could involve various technologies and expertise.

5.1 Scope

This section provides therefore, guidance for CABs-E on the attack methods that shall be considered in the context of the EIOT scheme for **security assurance Substantial Level**.

The attack potential mentioned in this document is largely inspired from [ISO-CC], **[CSPN]**, [GP TEE] and **[JIL-SMARTCARD]**.

Additionally, by describing the factors to be considered and by detailing examples of threats and full attacks, this document allows harmonization of conducted evaluation between CABs-E.

5.2 Covered Assets

The attack potential methodology will ensure the coverage of the following assets that are listed in SECTION 9 of the General Protection Profile **[TR-E-IOT-SCS-PART-2]** document.

Primary Assets:

- Device Data,
- Security Data,
- Configuration and Monitoring Data,

Secondary Assets:

- IoT End Devices (sensors and actuators),
- Communication Networks & Components (Networks, Protocols and the Gateway when it is part of the IoT End Devices,
- Software and Licenses (Operating System, Firmware and Mobile Applications for Extended TOE)

5.3 Preliminary partial and full attacks to be considered

It shall be particularly noticed that at the time of writing of this document, ENISA didn't have a specific list of attacks to be automatically considered in the context of a security assurance basic and substantial level. Nevertheless, and in order to anticipate the compliancy with ENISA's future work, the **[ENISA-BASELINE]** content is used and readapted as a base list of the threats and attacks.

5.3.1 Threats/Partial Attacks

The threat catalogue to be considered is listed in SECTION 10-COMMON THREATS and ANNEX V-THREATS CATALOGUE of the **GENERAL PROTECTION PROFILE [TR-E-IOT-SCS-PART-2]** document. The combination of these threats could lead to the full attacks that are described in section 5.3.2 Full attacks.

5.3.2 Full attacks

The minimum base list of full relevant attacks to be considered and that needs to be enriched with time is the one from the **[ENISA-BASELINE]** document. The attacks list is to be maintained and shall be able to fit in the attack's categories below:

1. Remote scalable attacks: all attacks coming from network interfaces and that a potentially could be scaled on several IoT connected device.
2. Software Attacks: all software attacks based,
3. Physical Attacks: all physical attacks based,

The Table 1 below illustrate the mapping between the ENISA's full attacks and these categories.

Full Attacks	Remote Scalable Attacks	Software Attacks	Physical Attacks
Against the network link between controller(s) and actuators	X		
Against sensors, modifying the values read by them or their threshold values and settings	X	X	
Ransomware	X	X	
Against the administration systems of IoT	X	X	
Power source manipulation and exploitation of vulnerabilities in data readings		X	X
Against actuators, modifying or sabotaging their normal settings	X	X	
DDoS using an IoT botnet	X		
Exploiting protocol vulnerabilities	X	X	
Against devices, injecting commands into the system console		X	
Steppingstone attacks		X	

Table 1:ENISA Full Attacks mapping

The table in Annex I detail for information the mapping between the ENISA's attacks and the threats/partial attacks listed above.

5.4 Determining attack potential

Similarly, to **[JIL-SMARTCARD]** and **[GP TEE]**, the calculation of the attack potential for IoT Device/Product makes the distinction between "Identification" and "Exploitation" phases.

Identification phase corresponds to the first creation of the attack (generally requiring most of the resource and skills of the attacker), while exploitation phase corresponds to the use of the identified/developed tools/techniques to perform the attack in the real operational environment of the IoT Device/Product.

As most of the attacks related to substantial assurance level are software oriented, splitting the identification and exploitation phases is particularly relevant. The first pilot projects will be determining how the adaptation will done for hardware attacks.

Attack methods calculation is mapped onto relevant factors similarly to the one specified in **[ISO-CC]**: Elapsed Time, Attacker's Expertise, Knowledge Necessary of TOE, Window of Opportunity and Equipment Needed. This document additionally introduces a new factor "Scalability" specified in section 5.5.6-Scalability p.29.

Finally, the attack potential of the attacker of the IoT Device/product is characterized as Low, Medium or High (For more details see section 5.6-Attack Potential Calculation Grid p.29). IoT device/products for substantial must resist to an attacker Medium potential.

Application Note
Substantial Assurance Level definition that is considered for the calculation attack potential: 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: • a review to demonstrate the **absence of publicly known vulnerabilities** and • 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.

5.5 Factors to be considered

Below is the list of factors that shall be considered by CABs-E when a full attack is identified during the evaluation. The attack potential grid shall appear in the Evaluation Technical Report described in section 6.3 p.31. The proposed preliminary factors' values and definition are to be enriched and completed during the pilot phase.

5.5.1 Elapsed time

The time spent by an attacker to identify, prepare, develop and exploit the attack.

It is considered as an assumption that evaluator is unlikely to spend more than 60 days attacking the TOE.

The amount of time is as follows:

- Less than one hour

- Less than one day
- Between one day and one week
- Between one week and one month
- Between one month and two months
- More than one month

5.5.2 Expertise

This factor represents the technical skills needed for an attacker in order to perform the attack. The different considered values are below:

- Layman: no particular expertise ("script kiddies")
- Proficient: familiar with IoT security behaviour, classical IoT attacks
- Expert: familiar with one of the following skills: implemented algorithms and IoT protocols (or cryptography), principles and concepts of IoT security, IoT techniques and IoT tools for the definition of new attacks including Well-known attacks, and reverse engineering, especially in an IoT operational environment.
- Multiple Expert: familiar with several software and hardware skills (these skills must be strictly different, e.g. reverse engineering and cryptography or Well-known attacks and cryptography...)

5.5.3 Knowledge of the TOE

This factor represents the knowledge needed by the attacker about the design of the IoT Device/Product considered as the TOE. It can be:

- Public: access to public information only (example: available on the Internet and other public resources and books)
- Restricted: access to information given by the vendor, with restricted diffusion (example: functional specification of the Device)
- Sensitive: access to information obtained by social or reverse engineering, (example: knowledge of the internal design)

5.5.4 Windows of Opportunity

Windows of opportunity factor as specified in **[ISO-CC]** refers to the access opportunity to the target product that is required for the attack and depends on the difficulty involved in accessing the product without the attack being noticed until it is successful:

- Unlimited access: no duration and quantitative restrictions
- Easy access: require access duration of about a day and/or very few samples (less than 10)
- Moderate access: require access duration of about a month and/or several samples (less than 100)
- Difficult access: require access duration for more than a month and/or significant samples (more than 100)
- Impossible: require access duration above the lifetime of the software product and/or a huge number of samples than cannot be obtained

5.5.5 Equipment

The software equipment required for exploitation of the attack. It can be:

- Standard: all software tools are available on Internet or at reasonable cost
- Specialized: all software tools are either costly or need some customized development to answer the IoT specificity (example: in order to attack specific protocols),
- Bespoke: all software tools are highly sophisticated, costly, and developed for a targeted application (example: to attack proprietary protocols and Operating Systems)

5.5.6 Scalability

The scalability is a new factor that is considered in the IoT environment and more specifically for the substantial security assurance level.

This factor will allow to represent the capability of an attacker to exploit the vulnerabilities in a large set of devices and geographical areas. The values are defined as follows:

- Easy: the attack is generic and thus can only be exploited on all or several range of IoT Device/Product,
- Moderate: the attack can only be exploited on a full range of category of the IoT Device/Product,
- Difficult: the attack can only be exploited on very few instances of a category/version of the IoT Device/Product

5.6 Attack Potential Calculation Grid

CAB-E will be able to generate the attack potential calculation grid for each full attack basing on the description of the factors in section 5.5.

The table below will make a correspondence between a factor and a numeric value in order to provide the global rating of the attack. This table is largely inspired from **[ISO-CC]**.

FACTOR	IDENTIFICATION	EXPLOITATION
	ELAPSED TIME	
<= 1 HOUR	To Be Defined	To Be Defined
<= 1 DAY	To Be Defined	To Be Defined
<= 1 WEEK	To Be Defined	To Be Defined
<= 1 MONTH	To Be Defined	To Be Defined
BETWEEN 1 MONTH AND 2 MONTHS	To Be Defined	To Be Defined
> MORE 2 MONTHS	To Be Defined	To Be Defined
	EXPERTISE	
LAYMAN	To Be Defined	To Be Defined
PROFICIENT	To Be Defined	To Be Defined
EXPERT	To Be Defined	To Be Defined
MULTIPLE EXPERT	To Be Defined	To Be Defined
	KNOWLEDGE OF THE TOE	

PUBLIC	To Be Defined	To Be Defined
RESTRICTIVE	To Be Defined	To Be Defined
SENSITIVE	To Be Defined	To Be Defined
	WINDOWS OF OPPORTUNITY	
UNLIMITED	To Be Defined	To Be Defined
EASY	To Be Defined	To Be Defined
MODERATE	To Be Defined	To Be Defined
DIFFICULT	To Be Defined	To Be Defined
IMPOSSIBLE	To Be Defined	To Be Defined
	EQUIPEMENT	
STANDARD	To Be Defined	To Be Defined
SPECIALIZED	To Be Defined	To Be Defined
BESPOKE	To Be Defined	To Be Defined
	SCALABILITY	
EASY	To Be Defined	To Be Defined
MODERATE	To Be Defined	To Be Defined
DIFFICULT	To Be Defined	To Be Defined

This calculation will allow to have the following ranges to be completed during the pilot evaluation phase.

SUM OF THE ATTACK POTENTIAL	RESISTANT TO AN ATTACKER WITH AN ATTACK POTENTIAL OF:	FUNCTION RESISTANCE LEVEL
TO BE DEFINED	**NO CLASSIFICATION**	
TO BE DEFINED	**LOW**	**BASIC / ELEMENTARY**
TO BE DEFINED	**MEDIUM**	**MEDIUM / AVERAGE**
TO BE DEFINED	**HIGH**	**HIGH**

6 EVALUATION OUTPUT

6.1 Objectives

The objective of this activity is to describe the Observation Report (OR), the Evaluation Technical Report (ETR), the IoT Metadata Certification Statement (MCST) and the Certificate that must be produced by the CABs at the end of each evaluation.

Consistent reporting of evaluation results facilitates the achievement of the universal principle of repeatability and reproducibility of results. The consistency covers the type and the amount of information reported. ETR and OR consistency among different evaluations is the responsibility of the CAB.

Note that those expected results must be reusable in between stakeholders which requires these to be structured in a specific way allowing the editor to extract “non-shareable” information.

The CAB-E performs the two following sub-activities in order to meet the requirements for the information content of reports:

6.2 Observation Report (OR)

For FAIL or INCONCLUSIVE verdicts, the CAB-E could advise the developer of issues requiring resolution or clarification within the evaluation evidence. This could be expressed in the Observation Report (OR) delivered to the vendor.

For NON-APPLICABLE verdicts, the CAB-E should explain and clarify the reasons in the report.

The CAB-E/reviewer assigns an overall PASS verdict to the SAA only when all of the work units for that component had been assigned a PASS verdict.

6.3 Evaluation Technical Report (ETR)

The e-IoT-SCS Evaluation Technical Report will be issued by CABs and will mostly be based on a template simplifying and harmonizing the work. I summarize the work done and the results of the assessment.

6.4 Security Assurance Activities Testing Template (SAATT)

CAB-E shall maintain the results of all the tests performed during the evaluation (conformity described in section 4.1 and vulnerability described in section 4.2) in the template format shown in Table 1.

This will allow to facilitate the exchanges between both CAB-R and CAB-E whenever it is necessary to have more information about a specific test. It will also allow to have a traceability about all the tests that potentially could be reused for a delta certification.

Security Functionality: ….	Test reference: …	Author: …
Dependency to another test(s): ….	Test Goal: …	
Test Procedure: …		
Test Case	Expected Results	Observed Results
…	…	…
Conclusion		
…		

Table 1: Security Assurance Activities Testing Conformity Template[15]

6.5 Security Profile Coverage (SPC)

The SPC represents the Security Profile that was used as a base to evaluate the ToE. This version of the SP will include the CAB-E’s results of the requirements coverage including public notes or recommendations if any.

[15] This template must of course recall the version of the ToE that is tested

This will provide end users and device suppliers with the right type of information summarizing the work done and the results of the assessment.

6.6 IoT Metadata Certification Statement (MCST)

The MCST is intended to provide an attestation for each certified IoT device if "Attestation" feature is supported.

This concept will allow service providers, vendors and end-users to attest the validity of the certificate. For instance, service providers would be able to enforce security policies relying on the CMS provided by the Vendor.

For more information on MCST refer to [TR-e-IoT-SCS-Part-8].

6.7 Certificate

Once the CAB-E reviewer finalizes his inspection of the results of the evaluation, he will produce the final certificate which should be publicly available. This should include at least the CABs (name, address, contact details, licence number), the label or mark of conformity, the ToE identification, certification number, version of the conformance documents used and the date of issuance.

The certificate issued by the CAB-R to the vendors must be the one recognized by the e-IoT-S Certification Scheme. The [TR-e-IoT-SCS-Part-9] document contains a template format for a typical certificate.

6.8 Mark/Label

A mark/label could be created for customer assurance and marketing purposes. This mark should attest the presence of a successful certification and should reference the SPC which could be consulted for more information.

6.9 Management of Evaluation Output

The CAB-E shall perform configuration control of all the Evaluation Outputs.

This implies that the CAB-E must be able to identify and locate at any time and is able to determine whether a specific version of a document is in the CAB-E's possession.

The CAB-E shall protect the ETRs, ORs, MCSTs and certificates from alteration or loss while it is in the CAB-E's possession.

6.9.1 Disposal

Scheme owner may wish to control the disposal of the certificates and MSs at the conclusion of an evaluation.

The disposal of the Evaluation Output should be achieved by their respective owners (CABs and Scheme Owner) for 30 years after the date of their issuance and must be destroyed afterwards.

6.9.2 Confidentiality

The ETR and ORs may include sensitive or proprietary information and therefore must be stored confidentially by the CAB.

The sponsor and CAB-E may mutually agree to additional requirements as long as these are consistent with the scheme.

7 DELTA & DERIVATIVE CERTIFICATION CONCEPTS

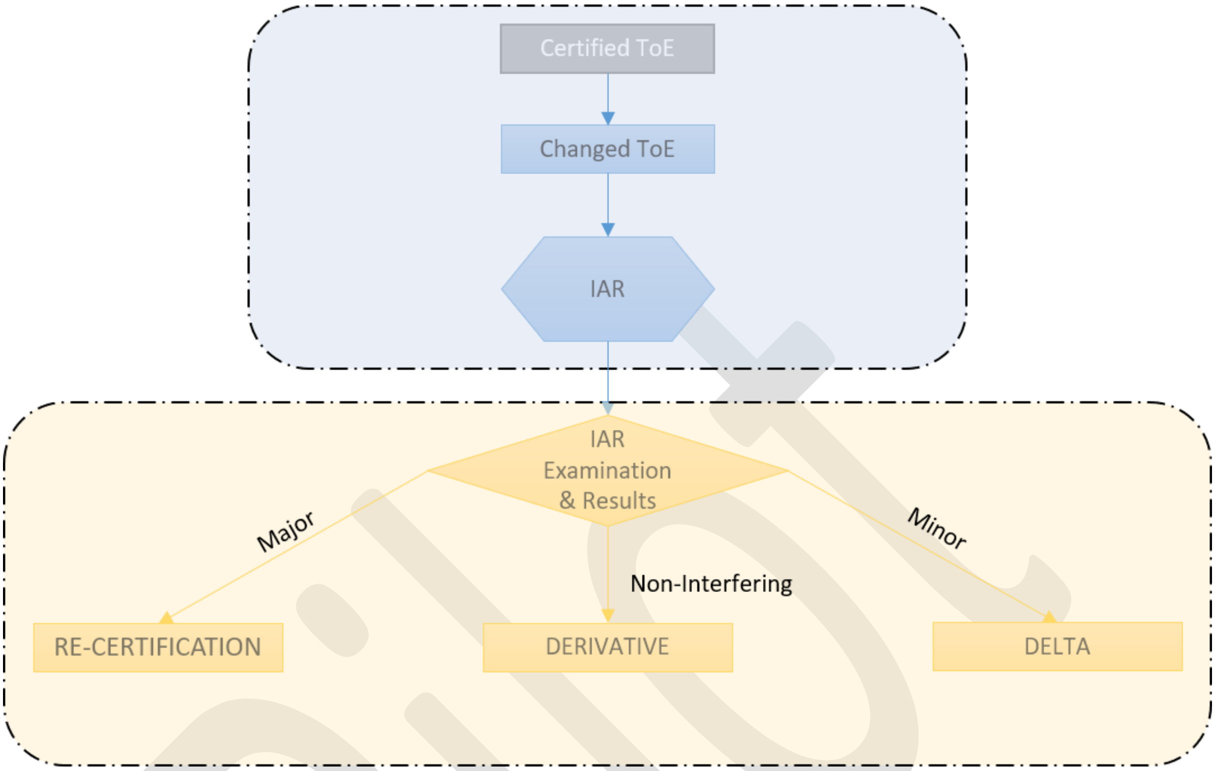

Figure 6: Impact Analysis Report - Delta & Derivative Concepts

The Delta & Derivative Certification are intended to simplify the maintenance of the certificate and minimize the costs when certifying a family of IoT devices. The criteria will be defined clearly allowing when it is possible a straightforward judgement on the nature of the changes. A “Major” change will require a full recertification, a “Non-Interfering (with the security requirements)” change will be required only a new stamp and a “Minor” change will require a Delta certification relying on existing artefacts.

This process will consider the vendor’s proven capabilities in processing vulnerability disclosure, upgrades and incident response. An Impact Assessment Process on the manufacturing side could simplify this task.

8 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.

9 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.

ANNEX I – ENISA's ATTACKS MAPPING WITH THREATS

Attacks	Threat ID	Threat Description
	T01.	Replay of data
Against the network link between controller(s) and actuators	T02.	Disclosure of data (stored, processed, transported)
	T03.	Manipulation or injection of data (stored, processed, transported)
	T04.	Deletion of data (stored, processed, transported)
	T07.	Compromise of personal data/sensitive info/ confidential info etc.
	T020.	Interfering radiation
Against sensors, modifying the values read by them or their threshold values and settings	T011.	Substandard, malicious or fake device components
Ransomware	T04.	Deletion of data (stored, processed, transported)
	T013.	Malicious access to device/system assets.
-	T05.	Vandalism or Theft of device, storage media, etc.
-	T06.	Loss of device, storage media, etc.
Against the administration systems of IoT	T08.	Unauthorized use or administration of devices & systems
	T013.	Malicious access to device/system assets.
Power source manipulation and exploitation of vulnerabilities in data readings	T09.	Physical access to operation workstation/devices by malicious external actor
	T014.	Failure or malfunction of the power supply
	T010.	Lack of organizational policies & Procedures
Against actuators, modifying or sabotaging their normal settings	T011.	Substandard, malicious or fake device components
	T021.	Network Denial of service

DDoS using an IoT botnet	T011.	Substandard, malicious or fake device components
	T021.	Network Denial of service
-	T012.	Regulatory Sanctions
Exploiting protocol vulnerabilities	T013.	Malicious access to device/system assets.
Against devices, injecting commands into the system console	T013.	Malicious access to device/system assets.
Steppingstone attacks	T013.	Malicious access to device/system assets.
-	T015.	Unavailability of communication systems
-	T016.	Failure or disruption of service providers
-	T017.	Failure of Internal information systems
-	T018.	Environmental disasters
-	T019.	Natural disasters
-	T022.	Intercepting compromising emissions