EUROSMART
The Voice of the Digital Security Industry

Technical Report

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

Evaluation Report Template

Beta – v1.0

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, Sreedevi Beena – Red Alert Labs, Ayman KHALIL – Red Alert Labs

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
22/02/2019	V0.1	Initial version created
08/03/2019	V0.9	Completed all the sections – Draft version ready for usage/final comments.
03/06/2019	V1.0	BETA RELEASE

1 Contents

2 Table of Figures

1 INTRODUCTION

This document defines the e-IoT-SCS Evaluation Report Template: scope and contents. This report must be completed by CAB[1]s while fulfilling an evaluation of an IoT device. 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.

The guidelines contained herein are intended to provide a common ground and language for the CABs to conduct Security Evaluations and provide consistent results following e-IoT-SCS Security Requirements and Evaluation Procedures.

1.1 Overview

Security Evaluation can be explained as a procedure for examining the security level of an IoT device, conducted by a third-party known as CABs against the security requirements defined by the e-IoT-SCS and the vendor questionnaire (VQ)[2] completed by the vendor.

In order to achieve greater comparability between evaluation results, evaluations should be performed within this e-IoT-SCS certification scheme as defined in the Process and Policy document **[TR-E-IOT-SCS-PART-1]** and **[TR-E-IOT-SCS-PART-2]** and the evaluation methodology must be in accordance with the **[TR-E-IOT-SCS-PART-3].**

The evaluator 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 vulnerability.

The evaluation is just one step in the procedure of certification, and the CAB Reviewer validates and approves the results of the evaluation stated in the Evaluation Report before issuing the certificate to the vendor.

A brief description of how to use this document is explained inside **'Usage Guidelines**' section1.11 of this document.

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.

[1] Conformity Assessment Body
[2] The Vendor Evidence of all activities & description regarding the ToE is completed inside Vendor Questionnaire.

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 17025]	General requirements for the competence of testing and calibration laboratories
[FER]	FIDO Evaluation Report, version 1.1, April 2018
[CCDB-2007-09-002]	ETR template for composite evaluation of Smart Cards and similar devices, September 2007, Version 1.0, Revision 1
[CSPN-Eval]	Methodology for Evaluation for a first level security certification https://www.ssi.gouv.fr/uploads/2015/01/methodology_for_evaluation_for_a_first_level_security_certification_en.pdf

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 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

Refer to **[TR-e-IoT-SCS-Part-1]**, Section 1.4

1.5 Abbreviations and Notations

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

1.6 Audience of this Document

The primary audience of this document is the CAB's, but it may be useful to all the parties involved in the certification program willing to acquire an in-depth knowledge or understanding regarding the Security Evaluation process.

The intermediate audience of this document, after it has been completed by the CAB Evaluator, will be the CAB Reviewer to validate the results and approve the report.

1.7 Support

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

1.8 Conformity & Copyright notice

This document must be strictly confidential for only the CAB 1 Evaluator, CAB 2 Reviewer, and the vendor who is concerned with the current evaluation.

1.9 Roles & Responsibilities

1.9.1 CAB 1 Evaluator

The evaluator performs the evaluation tasks required in the context of an evaluation: the evaluator 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.

1.9.2 CAB 2 Reviewer

Once all determination activities (review 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) 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.

When the outcome of the review is positive, a decision is made to grant certification by CAB. 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 (CAB 2 Reviewer).

1.9.3 Vendor, Sponsor, Developer

They must provide all the necessary evidences required for the evaluation and certification process.

1.10 Evaluation Report Instructions and Structure

This Evaluation Report must be completed by an Approved Evaluator of the CAB.

Once complete, the Evaluation Report must be distributed to the CAB Reviewer and the vendor.

This Evaluation Report consists of the following sections:

- Section 3– IoT device Identification
- Section 4– IoT device Overview
- Section 5- Evaluation Type and Level
- Section 6- Results of Evaluation
- Section 7 - Conclusion
- Section 8 - Evaluation Evidence

Approved Evaluators, please complete the remaining pages of this Evaluation Report during the Security Evaluation. Details on how to complete each section are included in this template and should be replaced with the details of the evaluation. The contact details regarding the CAB's will be available in the official website.

1.11 Usage Guidelines

This document must be completed based on the evaluation done, reviewed and sent securely using PGP encryption. This is done in order to protect the confidentiality of the sensitive information regarding the IoT device being evaluated.

There are instructions for carrying out the evaluation process, explained inside each corresponding section of the report. All the instructions are described inside separate boxes (A sample is illustrated in **Figure 1)** under the heading 'Evaluator Instructions'. It is obligatory that no modifications must be made to the instructions. All the Evaluator responses must be provided inside the Response boxes (see **Figure 2**), dedicated for it under each section.

The evaluator must give references to the documents reviewed without revealing the confidential information contained within that reference document or the document itself, inside the section 8 of this report.

Evaluator Instructions:
CAB's must provide here an overview of all the methods, techniques and tools used for the evaluation process and they may reference here the capabilities (e.g.: devices, resources, etc).

Figure 1 A sample Table of Instructions to the Evaluators

Evaluation Process
The following evaluation methodology was carried out: **1. At first, the evaluators have evaluated the Vendor Questionnaire and the additional evidences produced by the vendor.** **2. As a second step, the Observation Report with 'unsatisfactory' results were returned to the vendor for further clarifications.** **3. ……..**

Figure 2 A sample table of response

2 Evaluation Details

Evaluator Instructions:

Please complete the following details inside the corresponding tables.

2.1 CAB details

CAB Name :	
Evaluator(s) Name:	
Evaluation Reference:	
Evaluation Start Date :	
Evaluation End Date :	
Miscellaneous:	

2.2 IoT device details

Vendor Company Name:	
Vendor Contact Name:	
Vendor Contact Email:	
ID:	
Commercial Name:	
Device Specification:	
Device Version:	

3 IoT device Identification

Evaluator Instructions:
Provide any relevant details identifying the IoT device under evaluation: • Identification of the Hardware part; • Identification of the underlying Software Platform/OS (if applicable) • Identification of the Operational Environment, where the device is going to be used. • Identification of the network connectivity and the interfaces the device possess. Note that all the references must be easily understood by the audience. Please provide the description of all the complex references.

IoT Device Identification

4 IoT device Overview

4.1 Description of the architecture of the device

Evaluator Instruction:
This section of the Evaluation Report must present a high-level overview about the IoT device/ToE (Target of Evaluation), including a description of the components it possesses, and the main features of the device that are concerned with the evaluation process. This must include a description of the Hardware and the software parts the device is built with. It should briefly describe the IoT device and its operational usage-> The first step is to provide a diagram/description explaining the device's/ToE's physical and logical features. The main purpose of this step is to introduce specific concepts that might be necessary to understand by the subsequent sections of this Evaluation Report, as well as to define the scope of what is under evaluation. It all starts with an identification of the ToE, the assets to protect in Confidentiality, Integrity and Availability, with the specifics of the data flows between the various devices/Things and Mobile Application for instance and between the devices and the IoT Server. Also, this must include a description about the typical users (e.g.: non-technical, administrator, technical expert, etc) of the device and the assumptions/policies, mostly laid by the organisation, regarding the device.

An image has been depicted below in order to provide an idea about the high-level logical layer for an IoT Device which constitutes the Target of Evaluation (ToE) covered in this e-IoT-SCS Scheme.

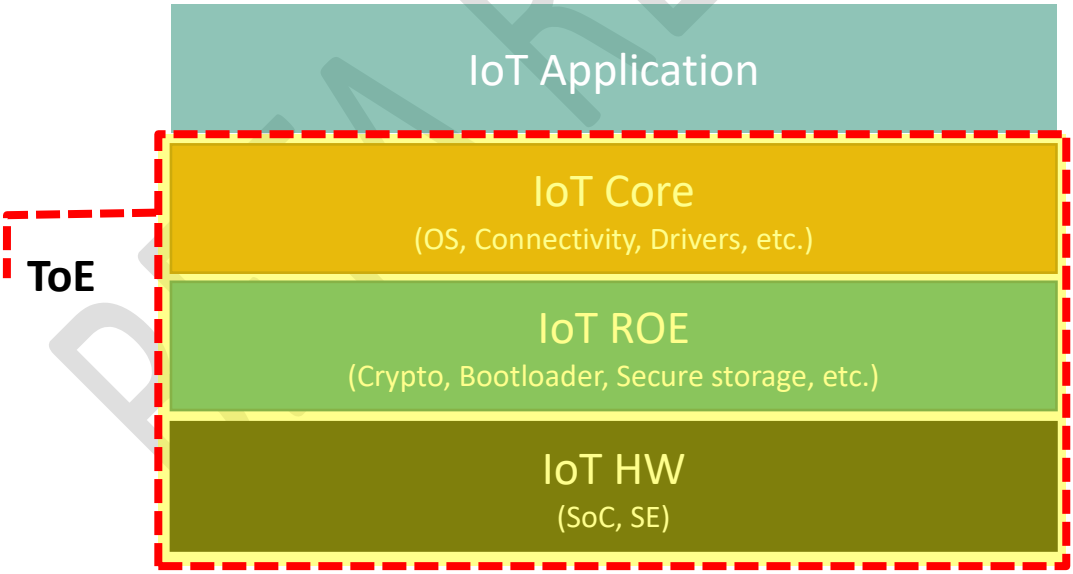

Figure 3 Target of Evaluation (ToE)

IoT device Architecture/ ToE

5 Evaluation Type and Level

The evaluation is the process of assessing the ToE against defined criteria. These criteria could consist for instance of source code review, documentation review, or black-box/grey-box /white-box testing. Manual Evaluation can be mixed with Automated Evaluation, for instance fuzzing or penetration testing tools.

The three types of evaluations are Primary Evaluation, Delta Evaluation and Composite Evaluation and the level is "Substantial".

- A **Primary Evaluation** requires the evaluation of the full scope of the IoT device from Hardware to Software.
- A **Delta Evaluation** is conducted on an already evaluated IoT device in its earlier versions. In such case, the CAB must review the Impact Analysis Report furnished by the vendor and must determine if any changes made in the new version is relevant to its security functionality used by the device to meet the security requirements. Only if the changes have an impact on the security functionality the CAB's need to provide this report and present the delta test results. If there are no changes, the CAB's can re-use the same evidences provided by the vendor to conduct the evaluation.
- A **Composite Evaluation** relies on existing certifications of underlying components (e.g.: ISO[3] certifications, Smart Card certifications) defined by e-IoT-SCS scheme. In this situation, the CAB's must conduct an evaluation of a part of the security functionality that the device cannot rely on the certified program to meet the security requirements as defined by the e-IoT-SCS scheme.

5.1 Methods, Techniques and Tools

Evaluator Instructions:
CAB's must provide here an overview of all the methods, techniques and tools used for the evaluation process and they may reference here the capabilities (e.g.: devices, resources, etc).

Methods, Techniques, and Tools

[3] International Organisation for Standardisation

5.2 Evaluation Constraints

Evaluator Instructions:
CAB's must report here inside this section, any conditions applied on the evaluation. This could be any type of assumption such as legal, confidentiality aspect, constraints on the distribution of evaluation result, etc, which could have an impact on the final evaluation results states inside this Evaluation Report.

Evaluation Constraints

5.3 Evaluation Process

Evaluator Instructions:
This section must include a description of the process methodology used by the evaluator while carrying out the evaluation (e.g. submitted incremental Observation Reports, failures addressed and then re-evaluated until the Evaluation Report passed completely, Impact Analysis Report submitted and Delta Evaluation process).

Evaluation Process

6 Results of Evaluation

This section presents the results of the evaluation. The results can be PASS, INCONCLUSIVE, FAIL or NON-APPLICABLE. The evaluator needs to verify all the evidences provided by the vendor and the developer, whether they are compliant with the specifications mentioned inside the **GENERAL PROTECTION PROFILE DOCUMENT [TR-E-IOT-SCS-PART-2]** and the **EVALUATION METHODOLOGY DOCUMENT [TR-E-IOT-SCS-PART-3]**.

For each of the following sections/domains, the CAB will provide the results for the following analysis requiring documentation review with clear justifications.

Evaluator Instructions:
Please provide the Evaluator's Results [4]and Rationale in each section below. Please give references to the documents reviewed without revealing the confidential information contained within the document or the actual document, inside the Evaluation Evidence of this report.

6.1 ToE Device Identification and Architecture

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the documents and additional references furnished by the vendor.

ToE Device Identification and Architecture
Result:

[4] It is important to note that CAB-E also maintain independently from the Evaluation Report the details of all the performed tests in conformity with the illustrated template in the 6.4 – SECURITY ASSURANCE ACTIVITIES TESTING TEMPLATE section of the **[TR-E-IOT-SCS-PART-3]** document. These tests templates are not integrated in the final report but could be used to provide more information in case needed following the evaluation phase.

Rationale:

6.2 ToE Users

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the documents and additional references furnished by the vendor.

ToE Users
Result:
Rationale:

6.3 ToE Operational Environment

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Operational Environment) and additional evidences furnished.

ToE Operational Environment
Result:
Rationale:

6.4 ToE Security Functionality

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Security Functionality) and additional evidences furnished.

ToE Security Functionality
Result:
Rationale:

6.5 ToE Functional Specification

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Functional Specification) and additional evidences furnished.

ToE Functional Specification

Result:
Rationale:

6.6 ToE Installation Guidelines

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Installation Guidelines) and additional evidences furnished.

ToE Installation Guidelines
Result:
Rationale:

6.7 ToE Flaw Remediation

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Flaw Remediation) and additional evidences furnished.

ToE Flaw Remediation
Result:

Rationale:

6.8 Device Life cycle process

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Device Life cycle process) and additional evidences furnished.

Device Life cycle process
Result:
Rationale:

6.9 ToE Integration

Evaluator Instructions:
Please provide the Evaluator's Results and Rationale after evaluating the response provided inside the Vendor Questionnaire (Integration) and additional evidences furnished.

ToE Integration
Result:

Rationale:

6.10 ToE Attack Potential

Evaluator Instructions:
CAB-E shall integrate the attack potential calculation grid for all identified full attacks in the context of the evaluation and according to the results. This is done according to the methodology described in SECTION 5 – ATTACK POTENTIAL CALCULATION GRID of the **EVALUATION METHODOLOGY [TR-E-IOT-SCS-PART-3] DOCUMENT**.

TOE ATTACK POTENTIAL FOR ONE IDENTIFIED ATTACK		
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

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

7 Conclusion

Evaluator Instructions:
This section outlines the overall verdict of the evaluation, which will relate to whether the IoT Device has satisfied the Security Requirements specified in the Security Profile of that device.> The rest of this section should outline sensitive aspects that should be analysed carefully. Provide any additional required information for a secure usage, or any additional information required for composite evaluation.

7.1 Observations

Observations

7.2 Recommendations

Recommendations

8 Evaluation Evidence

This section shall report for each element provided by the vendor and used as an evaluation evidence the following information:

- the vendor/developer/author name
- the title;
- the unique reference (e.g. issue date and version number)

Evaluation Evidence

9 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.

10 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