EUROSMART
The Voice of the Digital Security Industry

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

Impact Analysis Report

Template

Beta – v1.0

RELEASE

Editor: Sreedevi Beena – Red Alert Labs

Contributors & Reviewers: François Guerin – Thales, Alban Feraud – Idemia, Rachel Shabat – Winbond, 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

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
05/04/19	V0.1	Initial version created
28/05/19	V1.0	BETA RELEASE

1 Contents

1 INTRODUCTION

This document provides a template for the vendor who wishes to implement a change or modification in their product, production process or management system, which may affect the conformity of the product. In order to perform this, the first step they need to adopt is to inform the CAB-R. The CAB-R determines whether the announced changes require another initial testing and assessment or other further investigations. In such cases, the Vendor is not permitted to release products under the certificate resulting from such changes until the CAB-R has notified the Vendor accordingly.

Using this document, a Vendor wishing to extend the scope of certification to additional types or models of products[1], to the same specified requirements as the products for which a certification is already granted, applies to the CAB-R. In such cases, the CAB-R may decide not to carry out a full re-Certification but a Delta Certification.

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

A brief description about how to use this document has been explained under the section **'Usage guidelines'.**

1.1 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.

[1] Note that in case the ToE is extended to include the IoT application and Mobile application (please refer to the ToE extended definition in the **GPP [TR-E-IOT-SCS-PART-2]**) and the update is related to the application layer, patching with Integration mechanisms could be verified once by the CAB-R during the certification process. In that case, vendors can securely update the application while preserving the validity of the certificate.

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.

1.2 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.

1.2.1 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.

1.2.2 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

1.2.3 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.

1.2.4 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".

1.3 Terms and Definitions

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

1.4 Abbreviations and Notations

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

1.5 Audience of this Document

Vendors and CABs are the main audience of this document.

1.6 Support

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

2 Roles and Responsibilities

2.1 CAB Evaluator (CAB-E)

The evaluator performs the evaluation tasks required in the context of the evaluation : the evaluator receives the evaluation evidence (which possess the modification details and the result of impact analysis) 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 CAB Reviewer (CAB-R).

2.2 CAB Reviewer (CAB-R)

Once the evaluation is completed, the results are being reviewed by the CAB-R. If the evidence is sufficient, a recommendation for certification is made. This situation is similar to the procedure for acquiring first certification.

2.3 Vendor

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

3 Scope of Impact Analysis

Describe clearly the scope and purpose of the evaluation:

4 Usage Guidelines

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

The sections from 5 to 8 must be filled by the vendor who is seeking for the certification on the modified product. This information must include the result of impact analysis performed on each modification made. The CAB-E must evaluate the responses provided by the vendor along with the evidences furnished. The CAB-E must then provide their responses and results under section 9. There are response boxes provided under each section of modification, i.e., 9.1 and 9.2, which must be filled by the evaluator/reviewer. The instructions for completing the response boxes are also provided under

5 Contact information

Please complete the following details inside the corresponding tables.

5.1 CAB details

CAB-R Identification/Name :	
CAB-R Main Contact :	
CAB-E Identification/Name :	
CAB-E Main Contact :	
Evaluator(s) Name:	
Evaluation Identification:	
Certification Identification:	
Certification date:	
Miscellaneous:	

5.2 IoT Device Details

Vendor Company Name:	
Vendor Main Contact:	
Vendor Main Contact Email:	
IoT Device Identifier:	
IoT Device Commercial Name:	
IoT Device Complementary Information/Specification:	
IoT Device Version[2]:	
Certification Identifier:	
[Optional] Desired Certification end date:	

[2] Vendors could specify several hardware and software versions of the device (example: device hardware ID, Operating System ID, …)

6 Changes/Modifications- Hardware/Software

Certification Identifier	Changes (Specify Yes/No)	If Changes (Specify Hardware/Software)	Description of changes	Impact (Minor/Major/ Non-Interfering)

7 Changes/Modifications- Security Functional Requirements

Security Functional Requirements	Changes (specify Yes/No)	Description of changes	Impact (Minor/Major/ Non-Interfering)

8 Summary of changes

Software Changes (When Applicable)

Hardware changes (When Applicable)

Security Functional changes (When Applicable)

Other Changes

9 Results of evaluation

This section presents the results of the evaluation. The results can be PASS, INCONCLUSIVE or FAIL. 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-E will provide the results for the analysis requiring documentation review with clear justifications inside the following response tables.

9.1 Software/Hardware changes

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

Software/Hardware changes
Result:
Rationale:

9.2 Security Functional Requirements changes

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

Security Functional Requirements changes
Result:
Rationale:

10 References/Evidences

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)

Evidence

11 About us

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

12 Our members

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

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

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