EUROSMART
The Voice of the Digital Security Industry

Technical Report

[TR-e-IoT-SCS-Part-4]

GUIDELINES

Certification Agreement

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

EXECUTIVE SUMMARY

This document defines the guidelines for setting up a Certification Agreement and suggest a Template model to be completed by the parties involved in this agreement.

The primary entity getting involved in this agreement will be the CAB[1] (Conformity Assessment Body), who is responsible for conducting the evaluation and certification of IoT devices. The secondary party can be the stakeholders such as vendors or other CABs.

There are instructions for completing each section of the certification agreement. A brief description on how to use this document is explained under **'Usage Guidelines**' section of this document.

The guidelines specified inside this document have been prepared in accordance with **[ISO/IEC 17065:2012]** standard.

[1] The term CAB used in this document could be referring to either CAB-E (evaluator) or a CAB-R (reviewer)

Date	Version	Description of changes
22/10/2018	V0.1	Initial Template document
08/01/2019	V0.2	Contents added
29/03/2019	V0.3	Contents modified according to ISO 17065
28/05/2019	V1.0	BETA RELEASE

1 Contents

1 Introduction

These guidelines list the rules for setting up an agreement between CABs and Certification Scheme stakeholders (e.g. Vendors, other CABs).

The suggested content of a certification agreement includes information identified in **[ISO/IEC 17065:2012],** SECTION 4.1.2 taking into account some of this scheme key elements to adapt them to the use case while remaining consistent.

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.

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 General References

Reference	*Name/Description*
[ISO/IEC 17065:2012]	Conformity assessment — Requirements for bodies certifying products, processes and services

1.2.2 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.

1.2.3 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

1.2.4 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.

1.2.5 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".

1.3 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 Support

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

2 Usage Guidelines

This document must be completed by the parties who are involved in this certification agreement. There are instructions for filling out this agreement template. All the instructions are described inside separate boxes (A sample is illustrated in **Figure 1)** under the heading 'Instructions'. It is obligatory that no modifications must be made to the instructions. All the information regarding each section of this template must be provided inside the corresponding response boxes (see **Figure 2**), dedicated for it under each section.

Instructions
This section must be filled with the information regarding ……

Figure 1 Instructions box

Liability
The CAB must not have liabilities with the party getting involved in this agreement, during circumstances which can be accidental, unexpected, or intentional.

Figure 2 Response box

3 Recitals

Instructions
This section must state the role of the parties and the aim of the agreement: Company A representing CAB-E provides evaluation services and is able to carry out the duties described in this Agreement and Company B as a CAB-R/Vendor needs this service and is interested in contracting with Company A…

Recitals

4 Parties to the agreement:

Instructions
This section must be filled with the information regarding the parties that are getting involved in the certification agreement. The first box must be filled with the names and addresses of the parties involved and the second box must include the information about the authorized representatives, who are involved in the agreement.

— name and addresses of the parties

Name and address of the parties

— authorized representatives under the agreement

Authorized representatives under the agreement.

5 Defined terms and interpretations:

Instructions
There must be proper definitions for the terms and interpretations used inside the agreement. For example, the terms can be vendor, CAB, etc. The interpretations could be the assumptions. All those must be clearly defined inside this section.

— defined terms

Defined terms

— headings

Headings

6 Services to be provided

Instructions
Description of Business services
Services

7 Commitments of the client

Instructions
This section must include the commitments of the clients or the parties involved in the agreement who seeks for a certification. The client must comply with some of the requirements that are laid down by the certification body. The client may not be always the producer of the product, instead the client can be a distributer/importer. An example of the commitment (requirement) can be that 'the client always fulfils the requirements for certification, and it must readily make and implement the changes as and when communicated by the certification body'.

Commitments of the client

8 Use of license, certificates and marks of conformity

Instructions
This section must define all the criteria for licensing the CAB, the extent of usage of the certificates and marks of conformity. For example, the criteria for licensing could be that the CAB must be accredited by EUROSMART and/or a NAB, according to the specific requirements laid down. All clauses related to the usage of certificates and marks of conformity must be documented.

Use of license, certificates, and marks of conformity

9 Surveillance of certification

Instructions
This section must define the criteria and process for performing activities in order to carry out surveillance on the certification. This can include a periodic surveillance on the labels or marked products, by verifying whether the product still continues to satisfy the requirements for that certification. For example, assigning a person for reviewing the certification is an activity promoting the surveillance of certification.

Surveillance of certification

10 Suspension and withdrawal of certification

Instructions
All the actions to be taken during the event of suspension or withdrawal of a certification by the certification authority must be defined in this section. This must clearly include the information of the activities to be terminated immediately by the CAB or the party involved in the agreement. Also, the further steps to be taken in order to acquire the certification at the earliest, must be defined.

Suspension and withdrawal of certification

11 Complaints

Instructions
This section must be filled with the process to receive, evaluate and to make decisions on the complaints. This must also define the systematic approach undertaken by the certification body for recording the complaints received as well as the actions taken for solving it.

Complaints

12 Appeals

Instructions
In the event of withdrawal of certification by the certifying authority, the CAB has the right to appeal the decision. In this scenario, the conditions to be satisfied while appealing to the decision, to where the CAB must appeal, within what period of time, etc, must be defined inside this section of the agreement.

Appeals

13 Use of subcontractors

Instructions
All the terms and conditions regarding subcontracting must be defined inside this section. This must explain whether the party agrees with or does not agree with the notion of subcontracting or delegating to any third party any obligation in relation with any product under evaluation or is going to be evaluated. In any case, a written document proving the consent from the party involved in the agreement (vendors, other CABs, etc) must be obtained by the CAB.

Use of subcontractors

14 Changes by the client

Instructions
The information regarding whether the client has the right to modify the details of work performed or not, must be defined inside this section. This can also include situation such as modification or usage of the certified devices by the client. Generally, this is prohibited and is allowed only if there is a written consent by the certifying authority exists.

Changes by the client

15 Changes to the scheme and specified requirements

Instructions
Whenever there is a change in the scheme or specified requirements to be made, it must be in accordance with the clauses defined under this section. Both parties getting involved must agree upon these conditions. This must include the actions to be taken by both the parties when there is a necessity to modify the scheme or certain requirements followed.

Changes to the scheme and specified requirements

16 Transfer of certification

Instructions
This section must include the information regarding the transferability or non-transferability of certification by the CAB. Generally, the certification provided will be non-transferrable by the certified entity.

Transfer of certification

17 Fees and charges

Instructions
The CAB is required to maintain publicly the fees/charges they take for carrying out the certification activities. The medium can be electronic, paper etc. This section must be filled with the information about how it is publicised.

Fees and charges

18 Ownership of samples

Instructions
This section must define the clauses that are set forth regarding the ownership on samples provided for evaluation/certification. Normally, the CAB which has ownership on the device seeking certification, shall not be involved in its evaluation/testing process. This is to avoid any kind of partiality. All the conditions regarding this must be explained here.

Ownership of samples

19 Intellectual property:

Instructions
This section must include information on intellectual property such as: — vests in the certification body — ownership of pre-existing material — third-party material — moral rights — ownership of certification documentation and marks of conformity

Intellectual property

20 Confidentiality

Instructions
The criteria regarding the confidentiality of Information must be defined inside the agreement. This includes the usage of confidential information regarding the IoT device/product under evaluation or seeking certification by any personnel who is involved in the process. This must also explain the condition on the disclosure of these information. Normally, neither party can disclose any confidential information to any third-party unless they possess a written agreement for executing this. The CAB must define necessary restrictions on unauthorised use or disclosure of any confidential information in its possession during the term of the agreement.

Confidentiality

21 Insurance and liability

Instructions
The CABs must maintain and comply with the insurance requirements as specified inside the agreement. While defining this, all the laws regarding the region, that the CAB must comply with must also be specified. Proper clauses must be made regarding the liability or damages that could occur due to wilful misconduct of a party involved in the agreement. It must include all the circumstances such as accidental, direct, indirect, negligence, etc. The maximum limit of liability that a party can possess must also be defined inside the agreement.

Insurance and liability

22 Termination

Instructions
All the conditions regarding the termination must be defined. The CAB has the right to terminate the agreement at any time during the term, with or without cause, by providing a written notice prior to the day it intends to terminate. The agreement must explain the number of working days which the CAB must respect to give a notice. It must also specify the set of activities that will be terminated. The activities can include the evaluation processes, testing processes, etc. The effects of termination of the agreement must be explained clearly.

Termination

23 Force majeure

Instructions
The CAB must be free of any liability to the party involved in this agreement, in respect of any delay in executing the procedure for certification or testing, due to any exceptional situations such as fire, strikes, or any other type of disputes, governmental acts, which is not under the control of the CABs. The agreement must clearly explain the circumstances that has a vital role here.

Force majeure

24 Survival and severability

Instructions
To be defined accordingly

25 Dispute resolution

Instructions
All disputes claim or controversies that can arise in between the parties involved in this agreement must be resolved before the court specified under the Jurisdiction section of the agreement, which deals with the disputes arising. A reference must be made to the complete address of the court and regarding the rules of arbitration of the International Chamber of Commerce.

Dispute resolution

26 Alteration of this agreement

Instructions
The criteria for altering this agreement must be explained under this section. The agreements must never be amended without the prior knowledge of both the parties involved. The method of intimation must be in writing.

Alteration of this agreement

27 Serving notice under this agreement

Instructions
This section must define information regarding the deliverance of notices amongst parties involved in the agreement. For example, 'Any notices required or permitted by this agreement shall be in written format, whether it is sent by electronic mail or by postal'. The address to which the notices are to be sent must be clearly defined under this section.

Serving notice under this agreement

28 Governing law and jurisdiction

Instructions
The CAB must be compliant with all the applicable laws and regulations that are laid down regarding the import, export, or usage of the IoT devices that are submitted by the vendor to the CAB. This section must specify all the conditions that could affect the governing laws and must clearly mention the jurisdiction (the courts) where the CAB must go in the case of disputes. Additionally, there must be information on the regional law or regulations to which the CAB must adhere to.

Governing law and jurisdiction

28.1 Authorized representatives

Instructions
This section must be filled with the details about the authorized representatives who are getting involved in this certification agreement.

Authorized representatives

28.2 Services to be provided:

Instructions
This section must contain information about the services to be provided such as: — scheme name — specified requirements — products to be covered — locations of production to be covered

Services to be provided

28.3 Fees and charges:

Instructions
This section must contain information about: — general: Information about the fees and charges in general. — incidental expenses: The detailed information about the expenses that can occur in the event of dispute between the parties, must be documented inside the agreement. — invoicing and payment: Information about invoices and payments done.

Fees and charges

29 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.

30 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