

Technical Report

[TR-e-IoT-SCS-Part-7]

e-IoT MARK & CERTIFICATE

USAGE POLICY

Pilot — v1.2

RELEASE

Editor: Roland Atoui – Red Alert Labs

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

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
17/12/2018	V0.1	Initial version created
30/12/2018	V0.2	Described CABs usage policies, ...
31/12/2018	V0.3	Described Vendor's Usage policies
02/01/2019	V0.4	Described the Certificate Usage policy
22/03/2019	V0.5	Added the Certificate Template
31/05/2019	V1.0	BETA RELEASE
06/08/19	V1.0.1	Addition of BASIC level
21/10/19	V1.2	PILOT RELEASE

Table of Contents

1	INTRODUCTION	4
1.1.1	Disclaimer	4
1.2	Normative References.....	5
1.2.1	General References	5
1.2.2	Requirements & Evaluation.....	5
1.2.3	CABs Accreditation	5
1.2.4	Certification Secure Life-Cycle Management	6
1.2.5	Supporting Documents.....	6
1.3	Terms and Definitions	6
1.4	Abbreviations and Notations.....	6
1.5	Audience of this Document	6
1.6	Support	6
2	GUIDELINES/POLICIES FOR THE USAGE OF MARK	6
2.1	General	6
2.2	e-IoT-S CABs Usage.....	7
2.3	Vendor's Usage.....	7
3	SAMPLE SCENARIO FOR MARK USAGE POLICY	8
3.1	Policies.....	8
3.2	Specifications for MARK	9
4	GUIDELINES/POLICIES FOR THE USAGE OF CERTIFICATES	10
4.1	Certificates delivered to Vendors.....	10
4.2	Certificates delivered to CABs	10
5	About us	12
6	Our members.....	12
7	ANNEX	13

I INTRODUCTION

This document describes 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.

The Mark as it is defined in this document is a symbolical representation or identification, of a Certificate, which has been delivered to a vendor and uniquely identifies the certified product provided by them.

The rules/agreements made by this scheme owner or entities for the usage of these marks constitutes the “mark usage policies”.

I.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 TECHNICAL 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, INFORMATION, 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 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.

1.2.5 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 Audience of this Document

CAB-Rs, Vendors are the main audience for this document. They must follow the procedure and conditions which govern the use of the e-IoT BASIC and SUBSTANTIAL mark and certificate.

1.6 Support

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

2 GUIDELINES/POLICIES FOR THE USAGE OF MARK

2.1 General

- The **e-IoT-S** mark represents the Eurosmart **IoT Basic** and **Substantial** certificate delivered.

- The mark shall be displayed only in the appropriate form, size, and color detailed in [Section 3.2](#)
- These guidelines are applicable to the use of mark in any software, website, product packaging, product labels, promotional materials, licensing agreements, marketing and advertising materials, press releases, or other documentation.
- The ownership attribution should appear on the same page where the mark appears, if possible.
- The companies that gets involved in the usage of this mark should not mix it up along with their other marks. They must not use the same abbreviation that appears in the mark or certificate name, even if with the addition of few letters. For example, if the trademark name is “XYZ”, the vendor must not use it even if they modify it as “XYZCo” or “XYZLtd”.
- If a company uses the Mark without the proper consent of the owning authority, it does not imply that they have the authorization for using it or any approval on the products of that organization.
- When using the electronic form of the mark, it must be in accordance with the specifications.
- Upon any modifications to the e-IoT-S mark, the Scheme Owner must immediately inform the e-IoT-S CABs of its changes and proper use including the effective date.

2.2 e-IoT-S CABs Usage

- When an e-IoT-S CAB displays the mark in printed or online documentation, its accreditation license number issued by the National Accreditation Body (NAB) must appear under the mark.
- An e-IoT-S CAB shall not use the mark in any way that might mislead the reader regarding the status of the CAB accreditation or a specific vendor’s product certificate. For instance, the mark must be used only once the ToE passes the certification.
- An e-IoT-S CAB is intitled to use the nomination “e-IoT-S CAB” or to incorporate the e-IoT-S mark in public material referring to its conformity assessment services, provided that the conditions listed in this document are met.
- Any use of the e-IoT-SCS mark by a CAB that might contravene the conditions set out in this document will be subject to legal action which may include withdrawal of the e-IoT-S CAB license.
- Upon withdrawal of suspension of its accreditation by a NAB, an e-IoT-S CAB shall immediately cease to display or issue certificates and any other related materials displaying the e-IoT-S mark.

2.3 Vendor’s Usage

- IoT device vendors that have undergone certification by a CAB are authorized to display the e-IoT-S mark once the results of a successful conformity assessment according to the defined e-IoT-S criteria has been performed.
- After requesting a certificate, a legal agreement with the vendor to which this mark belongs to, must be signed. The legal agreement will specify the usage conditions according to these guidelines.

- The vendor's mark must appear in such a way that it should never overlap or get confused with the organisation's trademark.
- When a vendor uses or displays the e-IoT-S mark in printed or online documentation, the associated certification number issued by the e-IoT-S CAB shall be printed centrally under the mark in addition to the e-IoT-S Certification Scheme version.
- The e-IoT-S Mark can appear on a product "upgraded" version if and only if:
 - the product allows secure updates and
 - the flaw remediation validation was within the scope of the certification process.
 - the updates are not interfering with security functionalities in any way
 - or the vendors went through a Derivative or a Delta certification process.
- As specified in the [ISO/IEC 17065:2012] Conformity assessment — Requirements for bodies certifying products, processes and services, the consequences of transgressions by clients of CABs are managed by the CABs themselves.

3 SAMPLE SCENARIO FOR MARK USAGE POLICY

Let us consider a sample trademark, mark and the policies developed for its usage.



3.1 Policies

- The usage of the trademark ABCDTM must be in accordance with the legal agreement made with the organization.
- The trademark must appear on the first and the last page of the document (if it is used inside a document).
- All the occurrences of the trademark must accompany the notation "TM" with it.
- The ownership attribution must appear along with the trademark, in the first occurrence.
- Any addition or deletion of the letters contained inside the trademark, to denote any other aspect related to the vendor company is not allowed.
- The policies are applicable to all the means of usage (digital, hard copy, media, etc).

3.2 Specifications for MARK¹

- The allowed variations for the usage of mark are:



Letters in white with Red background

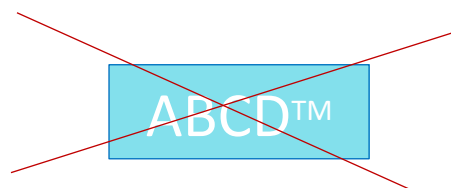


Letters in black with Yellow background



Letters in light blue with Dark Blue background

- Improper usage:



¹ To be replaced by the voted logo. See list in Annex



ABCD™

4 GUIDELINES/POLICIES FOR THE USAGE OF CERTIFICATES

4.1 Certificates delivered to Vendors

The certificate issued by the e-IoT-S CAB to the vendors must be the one recognized by the e-IoT-S Certification Scheme. The [\[TR-E-IOT-SCS-PART-9\] VENDOR CERTIFICATE TEMPLATE](#) document contains a template format for a typical certificate.



4.2 Certificates delivered to CABs

The certificate issued by the EUROSMART to the CABs must be the one recognized by the e-IoT-S Certification Scheme. The [\[TR-E-IOT-SCS-PART-9\] CAB CERTIFICATE TEMPLATE](#) document contains a template format for a typical certificate.

<h1>ACCREDITATION CERTIFICATE</h1>	
<p>THIS ACKNOWLEDGES THAT</p>	
<h2><u>Company X</u></h2>	
<p>IS ACCREDITED BY EUROS^{SMART} FOR CONDUCTING SECURITY <u>EVALUATION/</u> <u>CERTIFICATION</u> OF IOT DEVICES AGAINST E-IOT-S CERTIFICATION SCHEME</p>	
CAB Type	CAB-E or CAB-R
Level:	SUBSTANTIAL
Certificate Effective Date:	
Certificate Expiry Date:	
Certificate N°:	
<p><u>DIGITAL SIGNATURE</u></p>	
<p>EUROS^{SMART} The Voice of the Smart Security Industry</p>	
<p>ISSUED <u>APRIL 11, 2019</u></p>	

5 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.

6 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, Sanoia, 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

7 ANNEX

Logos proposed for voting



Figure 1: S14 Logo



Figure 2: S13 Logo



Figure 3: S12 Logo



Figure 4: S11 Logo



Figure 5: S10 Logo



Figure 6: S9 Logo



Figure 7: S8 Logo



Figure 8: S7 Logo



Figure 9: S6 Logo



Figure 10: S5 Logo



Figure 11: S4 Logo



Figure 12: S3 Logo

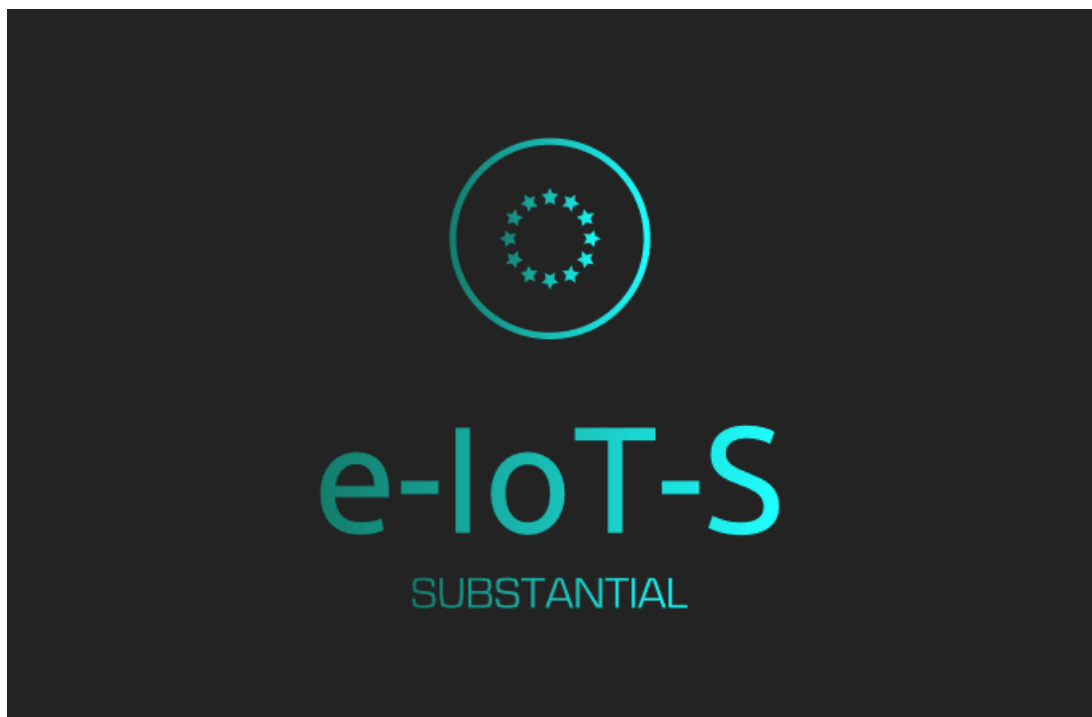


Figure 13: S2 Logo



Figure 14: S1 Logo