EUROSMART
The Voice of the Digital Security Industry

Technical Report

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

CAB Accreditation

Application Form

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
15/05/2019	V0.1	Initial version created
27/05/2019	V1.0	BETA - RELEASE

1 Contents

1 INTRODUCTION (Informative) 4
1.1 Overview 4
1.2 Disclaimer 4
1.3 Normative References 5
1.3.1 General References 5
1.3.2 Requirements & Evaluation 5
1.3.3 CABs Accreditation 6
1.3.4 Certification Secure Life-Cycle Management 6
1.3.5 Supporting Documents 6
1.4 Terms and Definitions 7
1.5 Abbreviations and Notations 7
1.6 Audience of this Document 7
1.7 Support 7
1.8 Scoring Criteria 7
1.9 Usage Guidelines 7
2 Application Form (To be completed) 9
2.1 CAB details 9
2.2 Proposed Scope of Accreditation 9
2.3 Business 10
2.4 Physical & Logical Security 10
2.5 Administrative Conformance 11
2.6 Technical Expertise 12
2.7 Surveillance Capabilities 14
3 Results and Recommendations (SECTION TO BE COMPLETED BY EUROSMART) 15
4 REFERENCES 17
5 About us 17
6 Our members 17

2 Table of Figures

Figure 1 A sample Table of Instructions for the CAB/NAB 8
Figure 2 A sample table of response for the CAB 8
Figure 3 A sample response table for the NAB to provide review response 8

1 INTRODUCTION (Informative)

This document defines the e-IoT-SCS Accreditation Application Form for CABs. This document must be completed by CAB[1]s seeking for an accreditation either to become a CAB-E (Evaluator) or a CAB-R (Reviewer).

The "CAB" term is used in this document to refer to either a CAB-E or a CAB-R unless it is explicitly mentioned.

The guidelines contained in Chapter 1 are intended to help the CABs in completing this application.

CABs must complete the Application Form presented in Chapter 2 and submit it to the Eurosmart.

1.1 Overview

In order to carry out the evaluation or the certification accurately, the CAB must get accredited at first under this scheme. The accreditation procedure takes place in accordance with the [TR-e-IoT-SCS-Part-5], ACCREDITATION POLICY - GUIDELINES document which explains the general requirements to be satisfied by the CAB seeking for an accreditation in order to conduct an evaluation on IoT devices, and the accreditation process in detail.

The entities which are particularly involved in this procedure are Eurosmart and the NAB[2], since they are the ones issuing the Accreditation.

Eurosmart will conduct a high-level review of the application and evidences furnished by the CAB in order to decide on whether to accredit the CAB or not. It is assumed that a NAB had conducted a complete audit based on the standards recognized by this scheme (e.g. **[ISO/IEC 17025], [ISO/IEC 17065:2012]**).

A brief description of how to use this document is explained inside **'Usage Guidelines'** section 1.9 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.

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

[1] Conformity Assessment Body (when used without extension CAB could be indicating either CAB-E or CAB-R
[2] National Accreditation Body

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 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
[ISO/IEC 17025]	General requirements for the competence of testing and calibration laboratories
[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

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 are the CABs and the NABs. The Application Form presented in Chapter 2 is intended to be completed by the CAB applying for an accreditation.

1.7 Support

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

1.8 Scoring Criteria

The Application will be scored for each requirement as follows:

- PASSED = The information provided by the lab sufficiently meets the requirement
- INCONCLUSIVE = The information provided by the lab is incomplete or not sufficient to meet the requirement.
- FAILED = The information provided does not meet the requirement.

For INCONCLUSIVE and FAILED results, the NAB will provide additional information as an informative recommendation.

A CAB must have all requirements as PASSED to be Approved by the NAB.

1.9 Usage Guidelines

CABs should complete all questions in this Application. If attachments are to be included with the application, please indicate the file name as [A-EVIDENCE-xx] DOCUMENT-NAME (xx being the unique number identifier e.g. [A-EVIDENCE-01] ISO17025 CERTIFICATE)

This document must be completed and sent back by email to Eurosmart: e-IoT-SCS@eurosmart.com securely using PGP encryption (Eurosmart's Public PGP key is available for download online). This is done in order to protect the confidentiality of the sensitive information regarding the CAB practices.

There are instructions for completing each section explained inside corresponding headings of the report. All the instructions are described inside separate boxes (A sample is illustrated in **Figure 1** A sample Table of Instructions for the CAB/NAB**)** under the heading 'Instruction'. It is obligatory that no modifications must be made to the instructions. All the responses from CABs must be provided inside the Response boxes for the CABs (see **Figure 2** A sample table of response for the CAB), dedicated for it under each section. All the review responses from the NAB must be provided inside the Response

boxes for the NAB under the section Results & Recommendations (see **Figure 3** A sample response table for the NAB to provide review response)

Instruction :
Please provide the evidence …….

Figure 1 A sample Table of Instructions for the CAB/NAB

Physical & Logical Security	
Physical and Logical Network security measures	**Our Lab maintains access control in the main entrance along with security alarms……**

Figure 2 A sample table of response for the CAB

Requirement Review	**Result**	**Recommendation**
Business Practices	**PASS**	**None**
Physical & Logical security	**INCONCLUSIVE**	**Please note that you must provide the certification evidence for……**

Figure 3 A sample response table for the NAB to provide review response

2 Application Form (To be completed)

2.1 CAB details

Instruction :
Please provide the following contact information inside the corresponding boxes:

Contact Information	
CAB's Name:	
Physical Address:	
Mailing Address:	
Zip Code :	
Country :	
Phone Number:	
Authorized Representative:	
Authorized Rep. Title:	
Authorized Rep. Email:	
Authorized Rep Phone:	

2.2 Proposed Scope of Accreditation

Please indicate the scope of Accreditation you wish to perform as an Accredited CAB:

Level	☐ Substantial
CAB Type	☐ CAB-E (Evaluator)
	☐ CAB-R (Reviewer)
Market Domain[3]	☐ Consumer
	☐ Enterprise
	☐ Industrial

[3] Multiple choices is allowed.

2.3 Business

Instruction :
Please provide the following evidence of business practices:

Business		
CAB Services		
Structure of the Organization (Including Design Area)		
Top 10 Vendors and percentage of revenue received for each Vendor relative to Total Revenue		
Certificate of Ownership and/or Tax Identification Number		

2.4 Physical & Logical Security

Instruction :
Please provide the following evidence of physical and logical security: Note: Evidence from other accreditation could be referenced hereafter (e.g. **[ISO/IEC 17025]**, **[ISO/IEC 17065:2012]**, CC Audit Reports, etc.

Physical & Logical Security	
Physical and Logical Network Security Measures	
Personnel Background Check Security Policies	
Confidential Data Protection Practices	

2.5 Administrative Conformance

Instruction :
Please provide the following evidence of administrative conformance: Note: Evidence from other accreditation could be referenced hereafter (e.g. **[ISO/IEC 17025]**, **[ISO/IEC 17065:2012]**, CC Audit Reports, etc.

Administrative Conformance	
Quality Assurance System	
CAB Personnel & Qualifications	

Proposed Approved Evaluators/Reviewers Note: At least one Approved Evaluator/Reviewer is required. Evaluators/Reviewers must complete the e-IoT-SCS Training for CABs and Knowledge Test to be considered Approved Evaluators. A CAB must have Accreditation from at least one of the programs mentioned inside [TR-e-IoT-SCS-Part-5] GUIDELINES ACCREDITATION POLICY and relevant to the CAB type (CAB-E or CAB-R)	
CAB Equipment and Techniques	
CAB Security Policy	
CAB Asset Management System	

2.6 Technical Expertise

Instruction :
Please provide the following evidence of technical expertise:

Technical Expertise		
Experience with IoT devices or similar HW/SW technologies (Please include statement of the evaluation projects, scope, and work carried out)		
Accreditation Program Evidence	Program	Date Received/Expiration Date

Provide the accreditation certificate provided by a NAB At least one of the following area of accreditations are required for a CAB-E: ○ [ISO/IEC 17025]- ITST ○ [ISO/IEC 17025]- IoT ○ PASSI and [ISO/IEC 17065:2012] ○ ANSSI-CSPN-AGR-P-01/1.2 ○ BSI-BCZ ○ NLNCSA-BSPA ○ NCSC-CPA ○ [Others…] At least one of the following area of accreditations are required for a CAB-R: • **[ISO/IEC 17065:2012]**		
Other Accreditations (Optional)		

2.7 Surveillance Capabilities

Instruction :
Please provide the following evidence related to your surveillance capabilities.

Surveillance Capabilities	
Describe your capabilities of conducting surveillance of the certified IoT devices as defined in SECTION 4.2 in the **[TR-E-IOT-SCS-PART-1] PROCESS AND POLICY** document of this Scheme.	
Acknowledge your part of responsibilities as defined in TABLE 1 - **[TR-E-IOT-SCS-PART-1].**	
Are you able to run an IoT Metadata Certification Service (MCSE)[4]?	

- **END OF APPLICATION** -

[4] The IoT Metadata Certification Service (MCSE) is a web-based tool where CABs can, on behalf of IoT device vendors, upload signed metadata statements for IoT service providers to access and use as a source of trusted information about a specific device model. Service Providers for IoT Devices will naturally want to be able to trust a device that attempts to make use of their services this makes the deployment of "device metadata service" very useful, secure and scalable in quickly determining if a specific device model is trustworthy to access a resource.

3 Results and Recommendations (SECTION TO BE COMPLETED BY EUROSMART)

Instruction :
This section will be completed by EUROSMART and returned to the CAB once the review of the Application is complete. The Application will be scored for each requirement as follows: • PASSED = The information provided by the lab sufficiently meets the requirement • INCONCLUSIVE = The information provided by the lab is incomplete or not sufficient to meet the requirement. • FAILED = The information provided does not meet the requirement. For INCONCLUSIVE and FAILED results, the NAB will provide additional information as an informative recommendation. The Application Result will be Approved or Rejected with Reasoning. When an Application is Rejected with Reasoning the CAB should review the recommendations provided and update the application as necessary and resubmit the Application.

Accreditation Reviewer details (EUROSMART)		
Name		
Email		
Date Review completed		
Requirements Review	**Result**	**Recommendation**
Scope of Accreditation		
Business Practices		
Physical & Logical Security		
Administrative Conformance		
Technical Expertise		

Surveillance Capabilities		
Application Result		

- **End of Results & Application –**

4 REFERENCES

Title	URL
[FIDO-LAB]	FIDO Certification CAB Accreditation Application, version 1.1, January 2018
[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
[TR-e-IoT-SCS-Part-5]	CAB Accreditation Policy - Guidelines
[TR-e-IoT-SCS-Part-1]	Certification Scheme Policy & Process
[TR-e-IoT-SCS-Part-2]	Generic Protection Profile
[TR-e-IoT-SCS-Part-3]	Evaluation Methodology

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**, **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.