EUROSMART
The Voice of the Digital Security Industry

# Technical Report

# [TR-e-IoT-SCS-part-5]

# CABs ACCREDITATION POLICY GUIDELINES

## Pilot – v1.2 RELEASE

**Editor**: Sreedevi Beena – 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, Roland Atoui – Red Alert Labs, Franck Sadmi – ANSSI, Jonathan Gimenez - ANSSI

**Approved by:** Martin Schaffer – SGS, Philippe Proust – Thales, Gisela Meister – G&D, John Boggie – NXP, Stefane Mouille – Cabinet Louis Reynaud

## EXECUTIVE SUMMARY

This document explains the general requirements to be satisfied by the CAB's[1] which seeks for an accreditation in order to conduct an evaluation on the IoT devices, and the accreditation process in detail.

Under this Scheme this document will be used mainly by EUROSMART as the Scheme Owner, since they are the ones issuing the Accreditation and hence, they need to follow the guidelines explained here while accrediting the CABs. It is also addressed for CABs undergoing an accreditation process to help them fulfil the accreditation requirements.

Under the Cybersecurity Act regulation, this document could be used a guideline or a template to be adapted to the relevant EU Cybersecurity Certification Scheme.

The accreditation process as explained inside this document focuses on the necessary aspects of a CAB to evaluate an IoT device and its various aspects related to its security.

All the CABs (CAB-E [2]and CAB-R[3]) shall follow the guidelines outlined in this document in order to apply for and maintain their Active status as an Accredited CAB.

The guidelines specified inside this document have been prepared in accordance with ISO/IEC 17025 and ISO/IEC 17065 standards.



[1] Conformity Assessment Body
[2] CAB Evaluator
[3] CAB Reviewer

| Date | Version | Description of changes |
|---|---|---|
| 22/10/2018 | V0.1 | Initial Template document |
| 01/03/2019 | V0.2 | Contents added |
| 28/03/2019 | V0.3 | Generic updates |
| 29/03/2019 | V0.4 | Security Experts and Peer review clarification |
| 27/05/2019 | V1.0 | BETA - RELEASE |
| 06/08/2019 | V1.0.1 | Addition of BASIC level |
| 26/09/2019 | V1.1 | Taking into accout ANSSI comments |
| 21/10/2019 | V1.2 | PILOT - RELEASE |

# 1 Contents

pilot

# 2 Introduction

These guidelines list the generic rules for accrediting CABs to be followed by EUROSMART for the administrative part and by the NAB for the full audit according to the relevant certification program.

It should be noted, that in addition to the NABs full audit accreditation process, a group of security experts must audit CABs on technical criteria. This group must ensure that the products and services are evaluated according to the methods defined by this certification scheme, and that the efforts and the technical expertise are in line with the expectations.

Facilities of the CAB used in product evaluation or certification must demonstrate to EUROSMART that they meet the applicable requirements listed in Section 3. This can be demonstrated by:

a) the CAB's facility having "already" an accreditation certificate fulfilling the CABs Accreditation Requirements with a scope of Evaluation or Certification covering the methods established by the Evaluation Methodology [TR-e-IoT-SCS-Part-3] for the product being certified; or

b) the assessment of the competence of the CAB by the NAB using a suitably competent Security Experts assessor, including the witnessing of Evaluation on a periodic basis; or

c) the CAB having a peer assessment recognition by the European Cybersecurity Certification Group (ECCG) with a scope covering the product being certified.

## 2.1 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.

## 2.2 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.

### 2.2.1 General References

| *Reference* | *Name/Description* |
|---|---|
| **[ISO/IEC 17000:2004]** | Conformity assessment — Vocabulary and general principles |
| **[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 |
| **[EU Cybersecurity Act]** | European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)) |
| **[ISO/IEC 15408]** | Common Criteria for Information Technology Security Evaluation (Part 1-3) |
| **[ISO/IEC 18045]** | Information technology -- Security techniques -- Methodology for IT security evaluation |
| **[ISO/IEC 17025]** | General requirements for the competence of testing and calibration laboratories |

### 2.2.2 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. |

### 2.2.3 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 |

### 2.2.4 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 & 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. |

### 2.2.5 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". |

## 2.3 Terms and Definitions

Refer to **[TR-E-IOT-SCS-PART-1]**, SECTION 1.4

## 2.4 Abbreviations and Notations

Refer to **[TR-E-IOT-SCS-PART-1]**, SECTION 1.5

## 2.5 Audience of this Document

All the CABs (CAB-E [4]and CAB-R[5]) shall follow the guidelines outlined in this document in order to apply for and maintain their Active status as an Accredited CAB.

## 2.6 Support

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

## 2.7 Roles & Responsibilities

### 2.7.1 CABs

A Conformity Assessment Body (CAB-E) (Evaluator) that has been accredited by a National Accreditation Body (NAB) is an organisation, which carries out Evaluations, independently from the developers of the ICT products. A CAB-R (Reviewer) is responsible for carrying out Certification and overseeing the day-to-day operation of an Evaluation.

| | |
|---|---|
| CAB (EVALUATOR) | The evaluator performs the evaluation tasks as specified in the Evaluation Methodology [TR-e-IoT-SCS-Part-3]: 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. |
| CAB (REVIEWER) | The Reviewer/Certifier reviews the work done by the evaluator and completes the Evaluation Report following the template provided in [TR-e-IoT-SCS-Part-9]. This report will be considered as part of the total package of evidence to demonstrate compliance with the certification requirements by the CAB's person or group responsible for making the certification decision.<br><br>Finally, the CAB issues the Certification. |

### 2.7.2 NABs

A National Accreditation Body (NAB) is responsible of CABs' accreditation (**with the support of the NCCA**) for one of the standard certification programs listed in Section 3 of this document. NABs are responsible of assessment and continued monitoring of the competence of CABs. NABs shall possess

[4] CAB Evaluator
[5] CAB Reviewer

the relevant knowledge, competence and means to properly perform audits to determine if a CAB has the technological knowledge, experience and the ability to carry out assessment.

### 2.7.3 EUROSMART[6]

EUROSMART is responsible of CABs' accreditation according to the e-IoT-SCS Accreditation Policy which is defined in this document. EUROSMART are responsible of the administration tasks defined in this policy in order to continually maintain the CABs accreditation.

### 2.7.4 Security Experts

Security Experts can be defined as a group of professionals who are responsible for verifying whether the CABs satisfy the requirements that are laid down in the certification scheme and the evaluation takes place in accordance with the certification scheme criteria and works in accordance with the standards specified such as ISO/IEC 17025.

This group must also carry out a security audit on the CABs on a regular basis, based on the technical criteria. These technical audits must also ensure that the methods, efforts, and expertise involved are homogeneous in all CABs operating in each Member State of the European Union. The experts in this group should be independent of the business entities involved in the certification scheme.

This group of security experts can be a recognised organisation that has expertise in the field of IoT security and the E-IoT-S Certification Scheme.

Experts in question could come from the NABs, its counterpart bodies, ECCG and ENISA, it could be also a designated competent CAB-R (reviewer)[7].

### 2.7.5 National Cybersecurity Certification Authority

National Cybersecurity Certification Authority (NCCA) main task is to implement and supervise some specific certification schemes covering ICT processes, products and services. NCCA should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories. Moreover, they should cooperate with other certification supervisory authorities or other public authorities by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.

NCCA are responsible for the accreditation of CABs in support to the NABs.

Peer Reviews are organised between Member States at the NCCA level.

### 2.7.6 EU Commission

The responsibility of EU Commission is to add the accredited CAB to the EU database.

[6] The role of EUROSMART could be completely replaced by NABs under the Cybersecurity Act regulation and recognition by ENISA.

[7] CAB-R will be designated eligible for auditing by EUROSMART/NAB on a case by case basis. CAB-R can only audit a CAB-E.

# 3 CABs Accreditation Requirements

Accreditation is granted following the successful completion of the Accreditation process which includes submission of an application, payment of fees, auditing, etc. The Accreditation is formalized through issuance of a Certification of Accreditation.

Compliance to ISO/IEC 17025 or ISO/IEC 17065 are a prerequisite requirement for all CABs. The scope must cover the Information Technology Security Testing (ITST) or the Internet of Things (IoT) domains.

## 3.1 CAB-E Accreditation Requirements

A CAB-E must have Accreditation from at least one of these programs:

| Scope | Program | Area of Accreditation |
|---|---|---|
| ISO/IEC 17025:2017 - ITST | Cryptographic and Security Testing | Basic Cryptographic and Security Testing<br>Cryptographic Modules - HW & SW Testing |
| ISO/IEC 17025:2017 - ITST | Common Criteria Testing | CC Testing |
| ISO/IEC 17025:2017 - IoT | IoT Device Testing [8] | IoT Device Testing |
| PASSI and ISO/IEC 17065:2012 | CERT CPS REF 33 | IT Security Audit Providers |
| ANSSI-CSPN-AGR-P-01/1.2 | LICENSING OF EVALUATION FACILITIES FOR THE FIRST LEVEL SECURITY CERTIFICATION in **FRANCE** | Hardware and Embedded Software / Secure Execution Environment / Digital Reception Terminal / Industrial Programmable Logical Controller. |
| BSI-BCZ | LICENSING OF EVALUATION FACILITIES FOR THE **GERMAN** BCZ CERTIFICATION SCHEME | IT Products |
| NLNCSA-BSPA | LICENSING OF EVALUATION FACILITIES FOR THE **NETHERLAND** BSPA CERTIFICATION SCHEME | IT Products |
| NCSC-CPA | LICENSING OF EVALUATION FACILITIES FOR THE **UK** CPA CERTIFICATION SCHEME | IT Products |

[8] Note that this scope is still not available, but this scheme assumes it will become a new standard domain

| | | |
|---|---|---|
| *[Others…]* | *"Other equivalent programs could be added on a case by case basis. "*[9] | |

## 3.2 CAB-R Accreditation Requirements

A CAB-R must have Accreditation from the following program:

| Scope | Program | Area of Accreditation |
|---|---|---|
| ISO/IEC 17065:2012 | Conformity assessment -- Requirements for bodies certifying products, processes and services | Information Technology Security Testing |

In addition to the elements assessed by NABs above, for the purposes of accreditation and this subject security expertise, it is considered appropriate to maintain at least the following elements:

- The legal status of the CAB organization and its group of membership and in particular the duty to inform in the event of significant modification (statutes, shareholders, managers ...);
- The commitment of a member of the management of the organization to apply the laws, directives and instructions relating to this activity and to inform the Authority in case of breaches or defective products (duty of care and information, participation in market surveillance);
- Participation in joint coordination bodies (approved organizations, authorities, standardization bodies, etc.) at the Member State or European level (Participation in experience feedback, capitalization, devolution of practices and interpretation of regulations).

## 3.3 Business Requirements

This section describes the overall business requirements which a CAB must meet.

### 3.3.1 Legal

The CAB's must be recognized as a legal entity and must be (or must be a part of) an organization that is registered as a tax-paying business or having a tax-exempt status or as a legal entity in some form with a national body. The CAB must be able to sign and abide by all the legal agreements for Accredited CABs, including [TR-e-IoT-SCS-Part-4] CAB Certification Agreement - Guidelines

### 3.3.2 Public Communications

The CAB agrees to abide by this certification scheme Process & Policy [TR-e-IoT-SCS-Part-1] that evaluation/or testing performed by the CABs is acceptable for only the certification of the IoT device and must make no claims to the contrary in its marketing material.

[9] CABs are invited to request an alternative equivalent program to be included to this list. In this case, EUROSMART/NAB will be responsible of consulting the security group experts and the scheme owner to validate or not such request.

### 3.3.3 Independence

The CAB must be able to perform the evaluations and testing independently, using its own analysis and Evaluation methodologies, which must be different from the ones defined by the vendor/ manufacturer of the device.

- The CAB must not be owned by the vendor who requests for the certification of their IoT device, without prior agreement.
- The CAB must never evaluate a device, on which they have been involved in the manufacturing/designing process, except that they may provide Quality assurance testing prior to the vendor submitting the product for official evaluation.

## 3.4 Security Requirements

This section describes the security requirements that a CAB must meet.

### 3.4.1 Physical

The CAB must maintain and follow certain physical security requirements as described in the following sections:

#### *3.4.1.1 Physical Layout*

The CAB must be physically isolated, allowing only the authorised personnel to enter the building. In order to accomplish this criteria, there must be adequate security measures in place to prevent the unauthorised from entering the building, especially in the case where the CAB is a part of another building or complex.

#### *3.4.1.2 Evaluation/Certification Areas*

The evaluation area where the IoT devices or its components or data are tested or stored must be isolated in such a way that it is restricted to authorized personnel (as per ISO/IEC 17025 or ISO/IEC 17065).

#### *3.4.1.3 Storage*

The storage space must be sufficient to provide adequate protection for all kinds of ongoing work. Secure storage must be provided for all materials retained by the CABs after evaluation has been completed.

### 3.4.2 Logical Security

The CAB must maintain and comply with a logical security policy that includes, at a minimum, the following requirements.

#### *3.4.2.1 Classified Materials and Information*

When handling the test samples, devices or evidence documents provided by the vendor, it must be handled with care and the materials must be controlled and stored securely, whether it is in electronic form or paper format.

Classified material must be stored in secure containers, where unauthorized access is prevented by appropriate measures (e.g. alarms, surveillance, and sufficient mechanical protection).

#### *3.4.2.2 Evaluation Reports*

All the Evaluation Reports must be stored securely. The CAB's must store all the confidential data (whether paper or electronic format) for at least three years from the date of evaluation. The

confidential data can be the documents and evidences provided by the vendor, the logs of the sessions of tests, etc.

When submitting electronic Evaluation Reports, the report must be PGP encrypted and securely uploaded. Evaluation Reports will be stored within an encrypted database only accessible by the CABs and will not be shared.

## 3.5 Administrative Requirements

This section describes the administrative requirements that a CAB must meet.

### 3.5.1 Quality Assurance

The CABs must have a quality system based upon ISO/IEC 17025 or ISO/IEC 17065 requirements, providing documented procedures defining processes to ensure a high quality of testing and test reproducibility.

### 3.5.2 Personnel

The CABs must maintain a list of their qualified test personnel, consisting of a description of their role in the organization, their qualifications, and their experience. The CAB must have procedures in place to ensure a match between staff training and roles in the performance of test activities.

The personnel performing the test activities/evaluation must be included inside the Evaluation Report, describing their roles and experience, while submitting the report. They must be approved evaluators and must possess knowledge on this certification program policies. In addition, the personnel must be capable of identifying any kind of deviation from the actual procedure for conducting the evaluation and test and should have the capability to reduce this deviation.

## 3.6 Technical Requirements

This section describes the technical requirements required for acquiring the accreditation.

### 3.6.1 Technical Expertise

Certifying IoT Devices at BASIC & SUBSTANTIAL level must be characterized by the fact that the type and scope of tests performed are predefined and correspond to the e-IoT-SCS Evaluation Methodology supported by this Scheme [TR-e-IoT-SCS-Part-3] describing the test methods and requirements applicable to the products in order to obtain their certification.

The CAB must possess an experience level of at least two years in the domain in which they are seeking for the accreditation. The CAB shall ensure that the staff have enough level of knowledge in carrying out the evaluations, the capability to address the deviations in the methodology used for evaluation, and to evaluate the significance of deviations. The CAB must maintain a record which details the competence of staff, the trainings they had, and the procedures for determining the competence required.

CABs must work on improving evaluation methods, so that the assurance gained during the initial certification process retains some of its validity on forthcoming updated versions (e.g. by evaluating the patch mechanisms on the product and patch processes from the developer), where evidence can be provided that those updates are issued according to a defined set of requirements.

# 4 CABs Accreditation Process

## 4.1 Accreditation Process

The following process is provided for indicative purposes to highlight some specificities to this scheme. Accreditation programs and processes are defined and managed by NABs.

| Step | Responsible Party | Process Requirement |
|---|---|---|
| **Accreditation Application** | CAB | Completes the *CABs Accreditation Application*. |
| | NAB | Completes review of *CAB Accreditation Application*.<br>Informs the CAB whether the Application meets requirements, by providing an Accreditation Application Report to the CAB |
| **Legal Agreements** | CAB | Sign legal agreement with the EUROSMART/NAB |
| **Accreditation Training** | CAB-R / EUROSMART | CAB-R / EUROSMART[10] to provide a one-day training for the CAB on the Certification Scheme.<br>A Knowledge Test must be performed by the end of the training |
| **Accreditation Issuance** | CAB | Pays Accreditation fees |
| | NAB & NCCA | If the Accreditation Assessment meets all requirements:<br>• (optionally) Signs a CAB Certification Agreement based on [TR-e-IoT-SCS-Part-4]<br>• Issues a CAB Accreditation Certificate. |
| | NCCA | Notifies about the accredited CAB to EU commission. |
| | EU Commission | Adds the accredited CAB to the EU database. |

[10] If this training should be provided to a CAB-R

# 5 Accreditation Application

In order to initiate the procedure for accreditation, the CABs must complete the Accreditation Application by providing evidence documentation for the topics covered by the sub-sections below.

CAB must fill-in the CAB Accreditation Application Form **[TR-e-IoT-SCS-Part-9]** before submitting it to the NAB.

## 5.1 Proposed Scope of Accreditation

This section describes those certification programs or levels within the programs for which the CAB is applying for Accreditation. This scope can be changed later following the Accreditation Scope Change process.

## 5.2 Authorized Representative

The CAB applying for accreditation, must designate an Authorised Representative that will act as the main contact for NAB.

## 5.3 Business Practices

The CAB should provide evidence of business practices in the form of a written report describing:

- Services of the organization
- Structure of the organization, demonstrating the isolation between the CAB and other areas of the organization (e.g. design area).
- Percentage of revenue received from each of the CAB's top ten vendor customers relative to the total revenue of the CAB.
- Certificate of ownership and/or tax identification number.

## 5.4 Physical & Logical Security

The CAB must provide solid evidence of physical and logical security. This must be provided as a written document or as part of describing the CAB procedures, which explains:

- The security policies implemented within the CAB in order to protect it physically and logically.
- Background checking policies implemented to verify the background of personnel.
- The data protection policies implemented concerning the confidentiality.

## 5.5 Administrative Conformance

The CABs must provide proper evidence of administrative conformance in the form of a written report describing:

- The Quality Assurance system maintained in the CAB laboratory.
- Details about the personnel working in the CAB including their qualifications, whether they are involved in the performance of any Evaluation or administrative duties connected with this Accreditation.
- Description about the equipment and techniques used within the CAB.

- Documentation on the security policies that are put in place, with special focus on the procedure for identification and recording of Evaluation samples or device components.
- Description on the Asset Management system for documentation and equipment.

# 6 Application Review

This section explains the procedure of reviewing the CAB Accreditation Application. During this step, the assessment is made by the NAB on whether the CAB fulfils all the applicable requirements within the proposed scope of Accreditation. The NAB will then inform the CAB by providing an Accreditation Assessment Report to the CAB, notifying if it may proceed with the Accreditation process.

# 7 Legal Agreements

## 7.1 Certification Agreement

The person or representative who is authorised must sign the Certification Agreement following the guidelines defined in **[TR-E-IOT-SCS-PART-4]**.

## 7.2 Confidentiality

No vendor, CAB, nor other third party may refer to a product, service, or facility as accredited, nor otherwise state or imply that NAB (or any agent of a NAB) has in whole or part approved, accredited, or certified a CAB or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions, and restrictions expressly set forth within an Accreditation Certification or Letter of Accreditation issued by the NAB or EUROSMART.

## 7.3 Consistent Business Practices

It is mandatory that any evaluation and/or test results from any CAB be recognized by all other Accredited CABs without any further investigation. In order to implement this, the "Peer Review" procedure could be practised.

A team of professionals (peer reviewers) could be deployed dedicatedly for carrying out this activity. Their job will be to understand the on-going activities for accreditation, review the activities carried out by the CABs and to document it periodically and provide a report at the end of each review.

Once this report is recorded and shared amongst other accredited CABs, it will be easier for them to be in tact with the on-going evaluations or test results obtained.

# 8 Accreditation Audit/Training

## 8.1 Audit

The CAB must perform internal audits at planned intervals in order to provide information on whether the management system is effectively implemented, maintained, and conforms to its own requirements set for the management system, including the activities going on in the CAB.

Apart from this, the CAB must define the audit criteria, the scope of each audit, implement corrective actions without delay (in the event of non-conformity) and retain records as evidence on the implementation of this audit activities and the results.

## 8.2 Training

Adequate training must be provided for the personnel who wish to become “Approved Evaluator” in the CAB. For the CAB to receive Accreditation, there is a requirement that at least one “Approved Evaluator” is a part of the CAB.

In the end, each evaluator must qualify the Knowledge Test provided by the end of the Training in order to become “Approved Evaluators”.

# 9 Accreditation Issuance

## 9.1 Fees

The CABs must pay all the Accreditation fees before an Accreditation Certificate will be issued.

## 9.2 CAB Accreditation Certificate Validity

The Accreditation Certificate issued to the CAB will be valid for a period of five years after the issuance date. It should be renewable on the same conditions provided that the CAB still meets the requirements.

NABs should restrict, suspend or revoke the accreditation of a CAB where the conditions for the accreditation have not been met or are no longer met, or where the CAB infringes the Cybersecurity Act regulation.

## 9.3 Decision Appeals

If EUROSMART/NAB decides not to issue an Accreditation, EUROSMART/NAB shall notify the CAB about the decision and will provide the reasons for not granting the Accreditation. If the CAB disagrees with the reasons provided for not granting the accreditation, the CAB may appeal the decision. Appeal actions shall be initiated within 30 days of the notification of the decision not to grant accreditation.

# 10 Accreditation Maintenance & Surveillance

## 10.1 Transparency of Evaluation Practices and Results

All the evaluation/certification activities should be documented. This must include, at least the Reference Devices used and the test configurations. All the rest of the information regarding the Evaluation shall be included as required in the Evaluation Technical Report. EUROSMART/NAB can any time demand for more information on how the test was conducted or reported, and the detailed records should be stored for a period of minimum three years from the date when the Evaluation Technical Report was submitted during certification.

## 10.2 Disclosure of Security Vulnerabilities

If at any time the CAB-E encounters a security vulnerability within the device, the CAB-E must immediately notify the CAB-R about this scenario and the vendor, at least within 48 hours. The vulnerability will be managed and handled as per the guidance documented in the **VULNERABILITY MANAGEMENT [TR-E-IOT-SCS-PART-6]** as part of this scheme.

## 10.3 Surveillance

All Accredited CABs must prove their capabilities to process surveillance activities as defined in SECTION 4.2 in the **[TR-E-IOT-SCS-PART-1] PROCESS AND POLICY DOCUMENT**.

CABs must also acknowledge their respective responsibilities defined in Table 1 in **[TR-E-IOT-SCS-PART-1]**.

## 10.4 Proficiency Assessments

At any time, at the discretion of EUROSMART or a NAB, a Proficiency Assessment shall be performed. EUROSMART/NAB will notify the CAB regarding the evaluation to be conducted on the Proficiency, the requirements of the assessment, and the date by which this must be completed. The scope of this Proficiency Assessment will include the CAB's capabilities and compliance with the CAB accreditation process.

If this assessment is not completed by the Accredited CAB with satisfaction, within the deadline specified by the NAB, the Accreditation may be revoked or suspended. A proficiency Assessment follows the process outlined in the Renewal Assessment (See Section 11.1), but the only difference is that, this is initiated by EUROSMART/NAB.

# 11 Accreditation Renewal

The CAB must be validated through a Renewal Assessment every 5 years to maintain the Accreditation.

## 11.1 Renewal Assessment

The Renewal Assessment must be completed before the expiration date of the CAB's Accreditation. It is the responsibility of the CAB to renew its Accreditation before it expires. If a CAB does not renew its Accreditation, EUROSMART/NAB may revoke its Accreditation.

| Responsible Party | Process Steps |
|---|---|
| **CAB** | Completes CABs Accreditation *Renewal Request* |
| **EUROSMART** | Completes assessment of the *Renewal Request*.<br><br>Informs CAB if the *Renewal Request* meets the requirements and if it may proceed with the Renewal process.<br>Identifies the Renewal Assessment requirements and informs the CAB |
| **CAB** | Schedules an appointment with a EUROSMART and makes the arrangements with the Security Secretariat for the Renewal Assessment.<br><br>Satisfactory completion of the Knowledge Test by at least one Approved Evaluator. |
| **EUROSMART** | Completes the *Renewal Assessment Report* and provides the document with the Approved or Rejected decision to the CAB. |
| | If the *Renewal Assessment Report* is Approved by EUROSMART. EUROSMART issues an updated *CAB Accreditation Certificate*. |

# 12 Modification or Termination of Accreditation

A CAB's accreditation may be modified or terminated. The following sections explains the reasons for modification or termination of Accreditation.

## 12.1 CAB Changes in Evaluation Services Offered

At any point of time, the CAB may decide to modify the services for Evaluation offered by it. In such case, the CAB is required to notify EUROSMART and the NAB about this.

If a CAB decides to cease offering one or more Evaluation services, the CAB must send a notice to NAB using 'Accreditation Change Request Form'. Upon reception of such request, the NAB will modify the CAB's scope of Accreditation accordingly. If applicable, EUROSMART/NAB will re-issue a new Accreditation Certificate, keeping the same expiration date as before.

## 12.2 CAB Changes – Other

The CABs must notify the NAB any time there is a change in the Evaluator who is a part of the CAB. The changes could be the person itself i.e., the Approved Evaluators, his/her legal status, location, or any other change that could influence the Accreditation. The CAB should use the Change Request to notify about these changes to EUROSMART and the NAB.

## 12.3 Accreditation Scope Change

If there is any change in the scope of the evaluation, i.e. to add a new Security Profile followed by a type of evaluation or testing, an Accreditation Scope Assessment is required. In any case, the existing date of renewal for the CAB's Accreditation does not change. The requirements for an Accreditation Scope Assessment are determined by EUROSMART/NAB at the time of assessment.

The Accreditation Scope Change process follows the Accreditation Assessment process, but instead by completing a Change Request.

## 12.4 CAB Termination of Accreditation

At any time, the CAB can request for the termination of the existing Evaluation Agreement with the NAB. For doing this, the CAB should complete an Accreditation Change Request to notify the NAB. Once this request is received, EUROSMART/NAB will confirm the termination of the Accreditation & Evaluation Agreement.

## 12.5 Non-conformance

This is a situation when the Accredited CAB fails to conform to the policies or requirements which were defined. If in case, EUROSMART/NAB discovers that a CAB is not in conformance with the policies laid down, EUROSMART/NAB will contact the CAB and will give a deadline for the CAB to correct the non-conformance or to provide further information. If the CAB fails to respond or is still not in conformance, the Accreditation will be suspended for further investigation or to allow the CAB to rectify their non-conformance. If the non-conformance is yet not solved, the Accreditation may be revoked.

If the CAB disagrees with EUROSMART's/NAB's decision, it may move forward for a formal appeal.

# 13 Accreditation Status

## 13.1 Pending

This status explains the situation when a CAB has started the Accreditation process but has not yet received an Accreditation certificate. Also, it has not received any notice regarding the decision taken not to accredit the CAB.

## 13.2 Active

The CAB has its Accreditation certification and it is alive.

## 13.3 Inactive

Due to some unavoidable circumstances, the accreditation status of the CAB has been placed on hold, which temporarily prevent the CAB from adhering the Accreditation policy.

The Inactive status for a CAB could last for not more than a year. But if this status continues to be Inactive for over a period of one year, the accreditation of that CAB shall be suspended.

## 13.4 Suspended

At any time, at the discretion of EUROSMART/NAB, it may suspend a CAB's accreditation:

- Based on the results of an assessment
- Due to CAB's non-conformance
- If a CAB fails to complete a Proficiency Assessment
- If the CAB is suspended:
- The CAB will receive written notice of the suspension along with the actions required to return to Active status.

The NAB will set the requirements and date by which a Proficiency test must be completed.

If the CAB remains in a suspended state for a period of 180 days, the CAB Accreditation will be Revoked. 90, 60, and 30 days prior to this deadline notices will be sent to the Suspended CAB.

## 13.5 Withdrawn

At any time, EUROSMART/NAB, at its discretion, may revoke/withdraw a CAB's accreditation:

- Based on the results of an assessment
- Due to non-conformance by the CAB
- If the CAB fails to renew its accreditation before the expiration date.
- If a CAB has not performed Evaluation on any IoT devices within the last three years.

If the accreditation is withdrawn:

- The CAB will receive written notice of the withdrawal.

- The evaluation agreement, which the CAB possesses, will be terminated.
- The CAB must furnish all the evaluation reports for IoT devices already certified or currently in Evaluation for certification within 30 days of the notice of withdrawal.

# 14 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.

# 15 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.