Joint Interpretation Library

Minimum ITSEF Requirements for Security Evaluations of Hardware Devices with Security Boxes

Version 1.1
August 2020

This page is intentionally left blank

Table of contents

1 Introduction

1.1. Background

1 The Common Criteria Evaluation Methodology [1] (see Annex A.5) describes the minimum work required for conducting a security evaluation and provides guidance for Certification Bodies (CB). This addresses activities or methods that go beyond the minimum level required for mutual recognition of evaluation results. One such matter that schemes may choose to specify is related to specific requirements in ensuring an evaluation was done sufficiently, so that every scheme has a means of verifying the technical competence of its evaluators. The main goal is to provide guidance to the Certification Body that all ITSEFs are adequate and comparable.

2 The SOG-IS-MRA requires Evaluation Facilities to be accredited according to the requirements of ISO 17025 [2], unless the Evaluation Facility has been established under a law or statutory instrument. Furthermore the SOG-IS-MRA requires Evaluation Facilities to demonstrate to the satisfaction of the CB, that it is technically competent in the specific field of IT security evaluation.

3 In the specific domain of hardware devices with security boxes (HWSB) the information provided in [2] does not provide enough detail to ensure that all the ITSEFs have the minimum set of equipment and skills to ensure credible results in their evaluations.

4 In order to harmonise this situation, a technical domain (within the framework of the SOG-IS agreement) has been created with the support and approval of the European Joint Interpretation Working Group (JIWG). This working group is responsible for harmonising the application of CC between the European Schemes. The role of the technical domain is to work on supporting documents concerning dedicated evaluation techniques such as penetration methods or so-called Attack Methods. These shall be implemented by the Certification Body claiming a qualifying status for specific IT technical domains.

1.2. Objective and scope

5 This document is intended to be one of the supporting documents of the evaluation process within the SOG-IS technical domain of hardware devices with security boxes [3]. [3] defines: “This IT-Technical Domain is related to products produced from a series of discrete parts on one or more printed circuit boards whereby significant proportions of the required security functionality depend upon a hardware physical envelope with counter-measures (a so-called “Security Box”) against direct physical attacks (for example payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals, Hardware Security Modules, etc.).”

6 The scope of the document is limited to the definition of the minimum capabilities that a SOG-IS accredited ITSEF should have in their premises to conduct the different types of attacks present in the Attack Method documents [4] + [11]. These capabilities include the knowledge and the skills of their evaluators and the necessary equipment to conduct the aforementioned attacks.

7 The capabilities are intended to cover the minimum requirements to perform the evaluation of the hardware, firmware and software of hardware devices with security boxes with sufficient guarantees.

8 In addition the SOG-IS accredited ITSEFs need the knowledge and the skills of their evaluators and the necessary equipment to conduct functional tests.

9 This document is not intended to provide guidance on how a hardware device with security box evaluation has to be performed, but it provides guidance to ensure ITSEFs have the necessary capabilities to conduct such evaluations. It does not describe how Certification Bodies examine that ITSEFs have the necessary capabilities to conduct such evaluations.

1.3. Target Audience

10 The target audience of this document are the Certification Bodies who plan to audit new and existing ITSEFs under the SOG-IS hardware devices with security boxes technical domain.

11 This document is also intended to be a reference for the ITSEFs that will conduct hardware device with security boxes evaluations and will be audited by their corresponding Certification Bodies.

2 Required Capabilities for a HWSB Physical Evaluation

2.1. Overview of a Physical Evaluation

12 The physical evaluation requires the development of specific skills and knowledge. The aim is to provide a technical guidance for evaluators running an evaluation and to expose the related minimum requirements.

13 To achieve this, the following sections will encompass:

- The understanding of the secure physical technology, its underlying principles and the development equipment used by manufacturers.
- The knowledge and experience in physical attack techniques that could compromise the hardware and an ability to use the related equipment to stress the hardware layers. This includes the understanding of the underlying physical principles.
- The ability to use the related equipment to conduct physical disruptions and the understanding of the related physical effects on the hardware.
- The knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture, signal processing procedures + analysis and rating).

14 The required tools for performing the various attack techniques can be categorised in standard (basic), specialised and bespoke.

2.2. Physical Technology

Evaluators must understand typical HWSB hardware and the underlying principles to the extent necessary to comprehend the design decisions of the manufacturer.

15 **Basic knowledge** is required of:

- the electrical behaviour of electronic components, e.g. resistors, capacitors, transistors, integrated circuits, RAM, ROM, E2PROM, etc.
- design principles of integrated circuits,
- chemical properties of typical HWSB hardware.

16 In addition, evaluators must have **detailed knowledge** of:

- microcontroller architecture, functionality and packaging,
- architecture and functionality of FPGAs (Field Programmable Gate Array) and ASICs (Application Specific Integrated Circuit),
- physical behaviour of removal and case opening detection switches,
- physical behaviour of sensors (temperature, voltage, …),
- layout principles of PCBs (Printed Circuit Boards),
- physical principles of protective shields (e.g. grid foils, printed grids),
- realisation of standard circuitry as used in micro-controllers,
- static and dynamic behaviour of digital and analogue circuitry,
- physical behaviour of potting mechanisms.

17 Evaluators must be able to understand the schematics (block diagrams, schematics).

18 Evaluators must have knowledge of the design process and must understand the process from the schematics (logical representation of the hardware) to the actual layout (physical representation). They must understand the processes of technology qualification, functional testing, characterisation, and reliability testing.

19 Evaluators must understand the development equipment used by the manufacturers for micro-controller software. This includes simulators, emulators, and special evaluation software tools. They must be able to read micro-controller source code and to develop software for penetration testing and other investigations. Therefore, evaluators must understand the CPU instruction set, the memory map and use of other peripheral units of the micro-controller.

2.3. Physical Specific Attacks

20 The following provides an overview about HWSB specific attacks. This is not a complete list but provides some examples. Detailed information about HWSB specific attacks in the context of CC evaluation can be found in [4] and [11].

21 Evaluators must have knowledge about standard attack scenarios and in principle be able to develop new ideas for such attacks.

22 To be more specific, evaluators must know about attack scenarios for HWSB such as intrusion of sensors, switches and filters, physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features and cryptographic attacks. A multitude of such attack scenarios – along with quotations – is described in the two JIL documents cited above.

23 Evaluators must be able to adapt and combine these attack scenarios for the individual HWSB being subject to evaluation. During vulnerability analysis they must be able to find possible weaknesses (in schematics and their realisation on the HWSB and the combination thereof) and be able to use the standard techniques to assess them.

24 Evaluators must have knowledge and experience of other HWSB attacks: side channel attacks (SCA) such as Timing Analysis, Machine Learning based SCA, Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential EM radiation Analysis (DEMA), Template Attacks (TA), fault injection attacks such as DFA and related attacks. The ITSEF must own or have unlimited access to the equipment (physical and analysis tools) necessary to perform such attacks according to section 2.4. The evaluators must be able to operate this equipment (including data-capture procedures) and to perform the analysis (mathematics). Knowledge and experience in cryptography and standard cryptographic attack techniques is required.

25 Evaluators must at least understand the physical principles, and the appropriate usage of the equipment classed as 'standard', 'specialised' and 'bespoke' as defined in [10].

2.4. Equipment for HWSB Physical Evaluation

26 In order to accomplish the vulnerability and failure analysis, physical manipulations and attack scenarios mentioned in section 2.3, the IT Security Evaluation Facility must have unlimited access to and own the majority of the tools of the category 'standard' and shall be able to use them efficiently.

27 The IT Security Evaluation Facility must have unlimited access to tools of the category 'specialized' and shall know how to use them efficiently.

28 Examples of this equipment and their categorisation are listed in [10].

29 The IT Security Evaluation Facility must at least possess a basic set of tools (unlimited access is not sufficient) for physical manipulations, side channel analysis, perturbation attacks and supply equipment. The supply equipment is needed for the operation of the TOE during the evaluation.

30 The basic set consists of the following tools:

- soldering iron, solder paste, heat guns, glue, needles, syringes, knives, steel cutting blades, screwdriver, hammer, standard drill, saws, dental toolkit (mirrors), tools for chemical etching, tools for grinding,
- multimeter, digital oscilloscope, signal/protocol analyser, PC or workstation, signal analysis software, shunts, wires and electrical probes, digital camera, endoscope, microphones, electric torch, antennas,
- voltage supply devices, signal and function generators.

3 Required Capabilities for a Logical HWSB Evaluation

3.1. HWSB Logical Design

31 Evaluators must understand typical HWSB logical architectures (e.g. the boot process, operating system, resource management and interfaces) and the underlying principles to the extent necessary to comprehend the design decisions of the HWSB developer. They must know the typical potential HWSB vulnerabilities and standard test and attack methods, especially domain-specific attack method papers [5] + [11].

32 Evaluators must show their ability to search for new publicly known vulnerabilities.

3.1.1 Source Code

33 A typical HWSB runs software on dedicated hardware. Therefore knowledge of software, how it is designed, compiled and executed and how it utilizes the hardware is important for the evaluation.

34 A wide array of programming languages can be used to write the software found in a HWSB. They can be categorized into three families:

- Low level: specific to the processor of the HWSB language (ARM assembler, x86 assembler, etc.),
- Intermediate level: compiled code (C, C++, ADA, GO, Rust etc.),
- High level: managed code, running inside a virtual machine or an interpreter (Java, Python, Shell, Perl, PHP etc.).

35 Now while assembler is less used, managed code, on the opposite, can often be encountered, as well as compiled code. Evaluators need a thorough understanding of the use of C/C++ or Java in the context of the specific hardware architecture. If the HWSB in evaluation or parts of it are programmed in other languages evaluators need a thorough understanding of these languages, too.

36 Moreover, for an in-depth security analysis, an understanding of assembler code and intermediate code (like Java Card byte code) is required. In particular, a variety of security impacts and defects cannot be understood on the level of a higher language like C or Java, because they become only apparent in assembler code or byte code. Therefore the importance of understanding assembler code produced by a compiler and security impacts of generation tools shall be explicitly emphasized – eventually the processor runs on assembler (machine) code, not C, Java or anything else.

37 In addition evaluators need to understand the impact of compilers, compiler libraries and interpreters on the security behaviour of the HWSBs in evaluation. They must know the meaning of the different compiler settings in relation to security aspects (e.g. if an optimization flag removes loops necessary to avoid timing attacks).

3.1.2 Interfaces

38 Evaluators shall be familiar with the different kind of interfaces which are typically used by HWSBs, e.g. Universal Serial Bus (USB), Serial, Ethernet port, Near Field Communication (NFC), Wi-Fi and Bluetooth. If a HWSB uses other kinds of interfaces they shall be familiar with them, too.

39 They must know if the interfaces allow potentially security-critical behaviour, e.g. direct memory access (DMA) or modes of operations which are not foreseen by the developer. Evaluators must know how to address the HWSB interfaces at the different ISO OSI layers and how to test their correct function.

40 They shall also be able, through software, to utilize debug ports available on the PCB, such as JTAG.

41 Evaluators must have knowledge of penetration tests related to the above mentioned interfaces.

3.1.3 Transport Layer Protocols

42 Evaluators must have knowledge of the security principles of the encryption schemes to be used for the transport layer protocols like secure messaging at smart card interfaces or TLS or SSH over the interfaces detailed in the above section.

43 Often these standards allow a high degree of flexibility in the configuration of security options, demanding scrutiny when evaluating a specific choice against a set of prerequisite requirements.

44 Evaluators must have knowledge of penetration tests related to the above mentioned transport layer protocols.

3.1.4 Application Layer Protocols

45 Evaluators must have knowledge of the security behaviour of application layer protocols, e.g. for POI knowledge of payment protocols like EPAS, IFSF (online) and EMV. Further examples are the processing of GNSS data in digital tachograph environment and the usage of the PACE protocol in smart meter gateways. The evaluators must know the security related state machines of these protocols as well as the underlying cryptographic mechanisms. They must be able to use test suites implementing such protocols to test security features of these protocols.

46 Evaluators must have knowledge of the typical PIN encryption schemes.

47 They must know the security principles of key management, HWSB management protocols and software download mechanisms.

3.1.5 Operating System, Content and Resource Management

48 The defining task of an operating system is the management of computational resources (like persistent and volatile memory, internal I/O, external interface components, display, keyboard, etc.) and the administration of access (interface) to such resources.

49 While the previous paragraphs dealt with the communication between a HWSB and the outside world, the focus shall lie here on the resource management *inside* the HWSB itself.

50 At first, evaluators need to understand the different types of operating systems and their specifics, e.g. a real-time OS will not behave the same way as a standard desktop OS. Also the file structure and file access rights administration within these various operating systems will differ. Knowledge of the memory types (EE, Flash, ROM, RAM), special dedicated RAM (like Crypto-RAM, Buffer-RAM) and memory management procedures (e.g. access limitations) are required.

51 The concept of domain separation and application isolation needs to be profoundly understood. This is especially relevant for application management, which refers to the secure loading, administration, deletion of application as well as the access rights of such applications to the HWSB's resources. This concept of separation is typically assisted by the underlying hardware/firmware platform, such as with the Trusted Execution Environment (TEE). It is important for the evaluator to have knowledge in this specific area.

52 The concept of boot-up processes for embedded devices, e.g. of multi-stage bootloaders, and the various possibilities of updating firmware and operating systems needs to be profoundly understood. Boot-up and update processes are potential targets for an attacker.

53 Another potential attack path might be the error handling e.g. in case of unexpected or misaligned expression as input. The evaluator must be able to analyse the error handling and to conduct appropriate tests.

3.1.6 Random Number Generator

54 The evaluator must have knowledge of and experience with evaluation methodologies for random number generators, in particular according to ISO/IEC 20543 [12].

55 For the evaluation of physical RNGs the evaluator must have sufficient knowledge in probability theory and design principles of physical RNGs. The evaluator must be able to identify and analyse those characteristics of a system or a process that have significant impact on the distribution of random numbers and to rate the randomness of number generation.

56 This analysis shall be quantified by a stochastic model. The stochastic model shall allow to verify a lower entropy bound per random bit. The stochastic model in particular comprises a family of distributions that contains the true (but unknown) distribution(s) of the raw random numbers (or at least of random numbers in an early stage of the generation process) during the life time of a physical RNG, even for defective states, e.g. unacceptable outputs. The stochastic model shall be justified by technical arguments. Furthermore, also the effectivity of online tests (also known as "health tests") shall be verified on the basis of the stochastic model.

3.2. Equipment for HWSB Logical Evaluation

57 In order to accomplish the vulnerability and failure analysis and attack scenarios mentioned in section 2.3, the IT Security Evaluation Facility must have

unrestricted access to the following categories of tools necessary to perform those analysis and attacks:

- Environment control equipment (e.g. to control communication, voltage, clock and temperature)
- Chemical and mechanical lab equipment (i.e. for sample preparation and analysis)
- Imaging equipment (e.g. cameras, microscopes)
- Logical test tools (e.g. for interface testing, vulnerability scanning, operating system testing, randomness analysis, source code analysis, circuit layout analysis, fuzzing tools)

58 Evaluators shall be able to operate the equipment to perform independent tests and attacks.

4 Life Cycle

59 Evaluators have to know the main phases of the life cycle which are the following: Development and manufacturing, initial software loading, delivery, installation and operation (including loading of software updates and additional software, end-of-life (e.g. controlled erasure of keys and destruction or re-use of hardware).

60 As an example the life cycle for POI is outlined in 4.1. The example shows in para 69 – 71 that the interpretation of the Common Criteria assurance components of the classes ASE, ADV, ATE and AVA might be required. Such interpretations shall be made in line with the Certification Body.

4.1. Example: POI Life Cycle

61 For POI evaluation evaluators have to know the main phases of the POI life cycle which are the following:

- Development and Manufacturing
- Initial Software and Cryptographic Key Loading
- Delivery
- Installation
- Acquirer Initialisation
- Use by Merchant and Customer

62 During manufacturing, the POI is assembled, powered on and tested (using the embedded software if present). Pre-personalisation is the manufacturing step if a POI receives the cryptographic keys to be used in the subsequent personalisation phase. In some cases, additional software is added to the embedded software at later phases of the POI life cycle. Software load agents are installed during initial software loading to allow further remote software installation, if applicable. The installation of a load agent uses the minimum load software present in the embedded software.

63 Initial cryptographic keys are loaded into the POI. Additional cryptographic keys can also be loaded during this phase. The POI is delivered at the end of the initial software and cryptographic key loading, which may be performed either by the terminal administrator through a terminal management system, either by the terminal manufacturer.

64 At the merchant premises, the POI performs card based payment transactions. POI administration is performed by an acquirer either through a connection to a terminal management system or directly at the POI. Further cryptographic keys may be loaded to personalise the POI.

65 POI installation and POI acquirer initialisation are pre-requisites to the use of the POI. These steps are performed at the merchant site using the user-accessible interfaces of the POI.

66 Installation depends on the configuration of the POI, either integrated in one enclosure or distributed. These steps may include:

- physical installation of the different POI components,

- cabling and connections to external peripherals which may be local, e.g. an Electronic Cash Register, or remote via an external access line,
- software downloading,
- configuration with specific parameters,
- mutual recognition of POI components (allowing components to exchange information, for instance in the context of a large retail configuration),
- test of the whole POI configuration and
- installation of the address of each acquirer and terminal administrator with whom the merchant has a contract.

67 Local operation on the POI is needed to start initialisation by the Acquirer. Acquirer initialisation takes place with each acquirer with whom the merchant operating the POI has a contract. Further cryptographic keys may be loaded during the acquirer initialisation to personalise the POI.

68 The acquirer downloads parameters configuring how transactions will be processed for each of the acquired brands. A merchant who does not want to get involved in the administration of his POI would put a terminal management system in charge of initialisation. Another merchant may put his own POI attendant in charge of initialisation. Sometimes, in preparation for acquirer address installation (POI installation steps) and for acquirer application configuration (acquirer initialisation steps), the POI receives the parameters that are common to the acquiring environments during the personalisation phase (e.g. list of active acquirers on the market with their initial host address, list of application identifiers and public keys of commonly accepted brands).

69 These examples show that a real development process can be more complex than the assumed one by the Common Criteria for conventional software or hardware products, since the complete life-cycle of a POI can be quite complex. Inputs and outputs are not always as simple as expected by the Common Criteria. As a result, the corresponding assurance components of the Common Criteria (for instance delivery) must be interpreted, refined, and rearranged if needed. In addition, it must be ensured that the processes of different components (and their description in terms of Common Criteria assurance components) fit together.

70 Evaluators must understand the POI development and supply chain and its integration into the application context in order to be able to interpret the Common Criteria assurance requirements in an appropriate way. In particular, these assurance requirements are:

- Guidance,
- Delivery,
- Installation, Generation and Start-Up,
- Tools and Techniques,
- Life-Cycle Definition, and
- Development Security.

71 In addition, differences between the evaluation of hardware and the evaluation of software means that the interpretation of the Common Criteria assurance components of the classes ASE, ADV, ATE and AVA is also required.

72 These interpretations of the Common Criteria assurance components and additional guidance are described in several CC Supporting Documents for POI published on the SOGIS website [7].

5 ITSEF Organisation

5.1. Quality

73 The IT-Security Evaluation Facility (ITSEF) must be well organised and provide instructions for the evaluators. These instructions must describe physical, procedural and organisational security measures or refer to other documents, where the information is detailed. A Quality Management System must exist. The requirements of ISO/IEC17025 must be met.

5.2. Subcontracting

74 When an ITSEF subcontracts work, this work shall be delegated to a competent subcontractor who is also a SOG-IS accredited ITSEF in the domain of hardware devices with security boxes. As such the subcontractor complies with the International Standard ISO/IEC 17025 for test labs and the personnel involved shall be technically competent for the related tasks and monitored by the lab licensing process of the responsible certification scheme. Subcontracting is not allowed to compensate for a lack of competence of the subcontracting ITSEF. The subcontracting ITSEF[1] must verify the competence and licensing status of the personnel of the subcontracted ITSEF[2] involved. The evaluation plan submitted to the CB for the individual evaluation project has to outline the subcontracted work and give a rationale of why the subcontracting ITSEF needs the support and why the external competences are needed. The subcontracted work must be performed under full control of the subcontracting ITSEF. The responsibility for the technical results provided by the subcontracted ITSEF is fully at the subcontracting ITSEF. For AVA activities only partial subcontracting is allowed.

75 Some attack methods for HWSB require specific chip know how and bespoke chip equipment, see e.g. section 2.3.3 + 2.3.4 in [5]. In that case this kind of work can be subcontracted to an SOG-IS ITSEF licensed in the technical domain for smartcards and similar devices. Requirements for SOG-IS licensed ITSEFs in the domain for smartcards and similar devices are described in [9].

5.3. Third party facilities and equipment

76 If the ITSEF uses other facilities (truly third parties meaning independent of both the ITSEF and the company/-ies developing and producing the TOE), appropriate

[1] The “subcontracting ITSEF“ is the ITSEF which subcontracts an other ITSEF.

[2] The “subcontracted ITSEF“ is the ITSEF which is subcontracted by the “subcontracting ITSEF“.

security measures must be applied to protect the vendor's information and samples and the know-how of the ITSEF. This may require additional measures if the TOE need to remain in the 3rd party facility unattended (overnight) or may require careful consideration for obtaining repeatability of test results if the sample has been removed from the site or the equipment settings modified prior to completing the TOE analysis. The use of the third party facility will have to be outlined in the evaluation plan and approved by the CB, while the ITSEF remains responsible for the work done.

77 If the ITSEF uses (bespoke) equipment at the third party facility, the evaluator must be present and must instruct the operating personnel. To instruct the operating personnel, evaluators must have sufficient knowledge of the TOE, the equipment, and the purpose of the test.

6 ITSEF assessment methodology

78 The ITSEF assessment methodology can be used at least for:

- Licensing of new Laboratory Company,
- Existing Security Evaluation Facilities that want to extend their licensing scope,
- Periodic assessments by the CB to maintain the ITSEF licence,
- Shadowing / voluntary periodic assessment within the SOG-IS mutual recognition agreement.

79 The CB will assess the Laboratory Company applying to be licensed on the basis of the following:

- Proof of Conformance – to the requirements stated in this document, initially by means of written evidence,
- Demonstration of capabilities – conducted as a site visit to audit the Laboratory’s physical environment, security procedures, quality assurance procedures, and test facilities, and to enable the Laboratory to demonstrate its capabilities,
- Pilot Security Evaluation – once the Laboratory Company has successfully demonstrated its capabilities, it performs a security evaluation in accordance with the rules of the scheme from which it is seeking licensing.

80 The following details the steps that need to be taken by a Laboratory Company wishing to become an ITSEF:

- Provide a security Self-Assessment and Conformance Statements to the requirements stated in this document to the CB,
- The licensing process begins with a review of the provided Statements and the CB might schedule an interview to obtain further clarification,
- The CB conducts an on-site audit of the Laboratory Company and as part of this audit:
  - The security Self-Assessment and Conformance Statements will be further evaluated,
  - The Laboratory Company must demonstrate testing capabilities.

- Upon successful completion of the on-site audit, the Laboratory Company is required to perform a "pilot" security evaluation. However, if findings are notified to the Laboratory, a corrective action plan shall be submitted and a follow-up assessment will be performed if applicable before entering the next step,
- Upon successful completion of the pilot security evaluation, the Laboratory Company becomes a licensed IT-Security Evaluation Facility of the CB where the licenses was applied.

6.1. Proof of Conformance

81 The Laboratory Company must provide written evidence of its conformance to:

- Administrative and Quality Assurance System conformance:
  - Formal accreditations or appropriate evidence related to approval based on national law, statutory instruments or an official administrative procedure,
  - Description of the Quality Assurance System including the procedures for identification and recording of test samples
  - A description of the laboratory security policy,
- Experience relevant to the desired Laboratory role:
  - A description of the Laboratory personnel and their qualifications through competence matrix and associated training plan,
  - A description of the overall Laboratory equipment, techniques and methodology documents.

82 Any subcontracting to a third-party entity must be declared in the abovementioned conformance statements and approved by the CB prior to the activity taking place. The CB reserves the right to audit these entities and to check the appropriate enforcement of the Laboratory’s security procedures specific to subcontracted activities.

6.2. Demonstration of capabilities

83 The assessment of ITSEF skills and capability can be performed in site visit of the ITSEF by Certification Body experts challenging the ITSEF experts and equipment based on the different attack classes of the Attack Method document.

84 The reference is the current Attack Method document at the time of the visit in order to cover the latest updated list of attack classes.

85 The goal of such a site visit is:

- To verify the written conformance statements made by the Laboratory to the Laboratory’s physical environment, security procedures, quality assurance procedures and test facilities,
- To assess whether the capabilities of the Laboratory and available equipment are state-of-the-art.

86 The CB will pay particular attention to the Laboratory’s detailed test procedures, and the evidence of its experience in the target domain.

7 Summary

87 This document has described the knowledge, skills and facilities required by an ITSEF before it can be capable of preparing and carrying out an evaluation of HWSB. These capabilities are not limited to having access to sophisticated types of equipment and the knowledge of how to use them. Moreover, ITSEF evaluators should completely comprehend the hardware device with security box design and production process and have the ability to develop and test for new attack scenarios. This knowledge cannot be gathered through short-term training but requires years of relevant experience.

88 If an ITSEF is known to meet the guidelines in this document, then a level of confidence will be provided to both the manufacturers (paying for the evaluation) and to the customers (accepting a certificate). Without these guidelines, that confidence can only be deduced by examining the detailed information from evaluation reports (although that still remains the ultimate measure of the ITSEF's performance).

8 Acronyms

CB	Certification Body
CC	Common Criteria
EMV	Europay, MasterCard and Visa
EPAS	Electronic Protocols Application Software
HWSB	Hardware Device with Security Box
IFSF	International Forecourt Standards Forum
ITSEF	IT-Security Evaluation Facility
JIWG	JIL (Joint Interpretation Library) Working Group
OSI	Open Systems Interconnection
PIN	Personal Identification Number
POI	Point of Interaction, Payment terminal
SOG-IS	Senior Officials Group Information Systems Security
SSH	Secure Shell
TLS	Transport Layer Security
TOE	Target of Evaluation

9 Bibliography

[1] **Common Criteria.** *Common Methodology for Information Technology Security Evaluation v3.1, Release 5,* April 2017.

[2] **ISO/IEC 17025:2017.** *General requirements for the competence of testing and calibration laboratories.* Corrected versions 2018-03 resp. 2018-04 for the French and the Spanish language. https://www.iso.org/standard/66912.html

[3] **SOG-IS.** *SOGIS - IT Technical Domain v0.93,* February 2011.

[4] **SOG-IS.** *Application of Attack Potential to POIs,* Version 1.0 (for trial use), 9th June 2011

[5] **SOG-IS.** *Attack Methods for POIs,* Version 1.0 (for trial use), 9th June 2011 (confidential document)

[6] **SOG-IS.** *Mutual Recognition Agreement of Information Technology Security Certificates V3.0,* January 2010

[7] **Common Criteria Portal.** http://www.commoncriteriaportal.org/cc/

[8] **SOG-IS-MRA-Portal**. https://www.sogis.eu/

[9] **SOG-IS.** *Minimum Lab Requirements for Security Evaluations of Smart cards and similar devices, Version 2.1,* February 2020

[10] **SOG-IS.** *Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0 (for trial use),* July 2020

[11] **SOG-IS.** *Attack Methods for Hardware Devices with Security Boxes, Version 3.0 (for trial use), February 2020* (confidential document)

[12] **ISO / IEC 20543:2019**: *Information Security - Security Techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408.* https://www.iso.org/standard/68296.html

The bibliography references the latest versions of the above-mentioned documents at the time of publication of the “Minimum ITSEF Requirements for Security Evaluations of Hardware Devices with Security Boxes” V1.1. When applying this paper the latest versions approved by SOG-IS / JIWG have to be applied. The latest approved versions are published on the portals [7] and [8] as far as they are not confidential or property of ISO/IEC.