Overview of ICT certification laboratories

FINAL

V1.1

JANUARY 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

ISBN: 978-92-9204-248-6
DOI: 10.2824/35439

Table of Contents

Executive Summary

Certification plays an important role in raising the level of trust and security in ICT products and services. This is also valid for new systems that make extensive use of digital technologies and which require a high level of security. National initiatives have been emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Important as they may be, they may nurture risks such as market fragmentation and challenges to interoperability.

This study seeks to identify and analyse the current landscape of ICT security certification laboratories in EU Member States, comparing them also with third countries practices. The findings of this study will constitute the basis for the Agency's proposal towards an EU wide ICT products and services certification framework.

Terms and their definitions are discussed in order to enable the identification of certification and/or evaluation models, and their instances usually called 'certification (evaluation) schemes' where respective entities can play different roles with different relations among them. To recognize equivalents, similarities and differences among terms in use, the following contexts are discussed: general normative, legal, specific normative and arranged.

The legal framework in the context of the certification of products can be seen on different levels as follows:

1. General requirements as set up by Regulation (EC) No 765/2008 of the European Parliament,
2. National level requirements from relevant accreditation bodies,
3. Certification or evaluation requirements from various standards,
4. Requirements resulting from international arrangements.

It has been found that in general, laboratories operate under respective national schemes. Although all are providing services of evaluating the security of ICT products based on an approved and unified methodology, their legal and business context varies, reflecting characteristics of local economies and policies of the Certification Body. By researching all licensed laboratories world-wide this report identifies relevant patterns, similarities and differences. The research will focus on the important implication from the European Union's perspective.

Standards used in the evaluation process include mainly ISO/IEC 15408-3 and ISO/IEC TR 18045. The main use of ISO/IEC 15408 is to assess the security of IT products. There are direct relationships between ISO/IEC 15408-3 assurance structure and the structure of evaluation process as described in ISO/IEC TR 18045. The ISO/IEC TR 18045 provides a description of evaluation process in terms of: roles and responsibilities and general evaluation model.

The evaluation according to Common Criteria usually happens in a typical ping-pong run. Evaluations are organized by examining several assurance classes separately. By the time this report has been prepared (November 2017) a total of 1864 certificates have been reported under www.commoncriteriaportal.org (main portal for CC certification) by European laboratories (around 150 per year). It falls into the responsibility of the certification body to ensure that evaluation labs meet the requirements. This includes competence requirements for evaluators. In this context, some certification authorities also have documented criteria that summarize the requirements.

1. Introduction and scope

Today's societies and economies are based on Information and Communication Technologies (ICT). Digitalisation increases cyber security risk across many sectors. There is a need to minimize the risk inherent in the use of ICT in society and the economy. One of the ways to achieve this is through ICT product certification. The certification obligations are implied by existing EU legislations; by the market needs, the industry, and ICT risk owners' expectations.

Certification plays an important role in raising the level of trust and security in ICT products and services. This is also valid for new systems that make extensive use of digital technologies and which require a high level of security. National initiatives have been emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Important as they may be, they may nurture risks such as market fragmentation and challenges to interoperability.

Taking due account of recent legislative and policy developments, such as the adoption of the NIS directive[1], publication of the European Commission (EC) position on the cPPP[2], and most importantly, the draft proposal of the EU Cybersecurity Act[3] ENISA continues to support the EC and the Member States in developing a certification framework for ICT security products and services, which on one hand will boost competition, and on the other promote mutual recognition of certificates and harmonisation of certification practices up to defined levels.

This study identifies and analyses the current landscape of ICT security certification laboratories in EU Member States, comparing them also with third countries' practices. The findings of this study will constitute the basis for the Agency's proposal towards an EU wide ICT products and services certification framework.

In the following sections, several aspects of the functioning of certification laboratories for ICT products will be described and analysed:

- Terms and definitions
- Legal framework
- Organisation of laboratories
- Standards used in the evaluation process
- Practices of laboratories

[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[2] https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-cppp-and-accompanying-measures
[3] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

2. Terms and definitions

2.1 Introduction

Discussing terms and their definition enables the identification of certification and/or evaluation models, and their instances usually called 'certification (evaluation) schemes' where respective entities can play different roles with different relations among them. Furthermore, it helps to recognize equivalents, similarities and differences among the terms in use depending on various contexts.

To recognize:

A. equivalents – i.e. terms having the same meaning regardless the context,
B. similarities –i.e. terms relevant for a particular scheme while their meanings can be considered as narrowing the context, and
C. differences – i.e. terms relevant for a particular context only, or the same terms of different meanings,

this chapter discusses the following context:

1. general normative – introduced by the ISO harmonized standards specifying broad context for conformity assessment activities performed by organizations with defined roles and responsibilities,
2. legal - as introduced by the Regulation 765/2008 as a conformity assessment framework,
3. specific normative – introduced by international standards i.e. ISO/IEC 15408 series and ISO/IEC 18045 (called hereinafter Common Criteria or CC), with regards to security evaluation and certification of IT products,
4. arranged –introduced in international arrangements i.e. CCRA and SOGIS-MRA, containing more detailed requirements, as agreed among the parties of these arrangements.

Set of relevant terms and definitions followed by illustration of relevant models are presented in clauses 2.2 -2.5. Then, clause 2.6 of this chapter will identify equivalents, similarities and differences between relevant terms.

2.2 General normative context

The primary concept of conformity assessment has been established in ISO's series of international standards, in particular, EN ISO/IEC 17000:2004, EN ISO/IEC 17065:2012 and EN ISO/IEC 17025:2017 (mentioning of a publication is a designation of the most recent version of a standard).

The defined approach - which is called hereafter 'General normative context' - refers to a concept of conformity assessment to specific requirements. It is described further by attestation activities which lead to a clear statement of conformity for a given product or service. Such a result could be achieved by using organizations, rules, procedures and management.

Terms and respective definitions for this general normative context are presented in the tables below. The first table shows the general conformity assessment environment (see Table 1).

TERM	DEFINITION
concept:	
conformity assessment	demonstration that **specified requirements** relating to a product, process, system, person or body are fulfilled
specified requirements	need or expectation that is stated Note 1 to entry: Specified requirements may be stated in normative documents such as regulations, standards and technical specifications
organization:	
accreditation body	authoritative body that performs **accreditation**
conformity assessment body	body that performs **conformity assessment** services
conformity assessment system	rules, procedures, and management for carrying out **conformity assessment**
conformity assessment scheme	**conformity assessment system** related **to specified objects of conformity assessment**, to which the same **specified requirements, specific rules and procedures** apply
agreement group	bodies that are signatories to the agreement on which an arrangement is based
activities:	
peer assessment	assessment of a body against **specified requirements** by representatives of other bodies in, or candidates for, an agreement group

Table 1: General normative context for conformity assessment based on the ISO 17000

By introducing the concept of 'attestation' one can narrow the conformity assessment context to a certification context by defining more specifically:

- organizations i.e. certification bodies (operating certification schemes) and laboratories (performing some of the conformity assessment activities needed to demonstrate the conformity with specified requirements by a given product or service), and
- activities i.e. certification and evaluation.

In such arrangements results of all conformity assessments are presented in the form of a statement issued by the respective body showing clearly the scope and relations in a given conformity assessment scheme.

This part of the general normative concept is presented in Table 2.

TERM	DEFINITION	SOURCE
concept:		
attestation	issue of a statement, based on a decision following **review**, that fulfilment of **specified requirements** has been demonstrated Note 1 to entry: The resulting statement, referred to in this International Standard as a "statement of conformity", conveys the assurance that the specified requirements have been fulfilled. (..)	ISO/IEC 17000
certification body	third-party **conformity assessment body** operating certification schemes Note 1 to entry: A certification body can be non-governmental or governmental (with or without regulatory authority).	ISO/IEC 17065
certification scheme	certification system related to specified products, to which the same **specified requirements**, specific rules and procedures apply Note 2 to entry: A "certification system" is a "conformity assessment system", which is defined in ISO/IEC 17000:2004.	ISO/IEC 17065
laboratory	body that performs one or more of the following activities: – calibration – testing – sampling, associated with subsequent calibration or testing	ISO/IEC 17025
activities:		
accreditation	third-party **attestation** related to a **conformity assessment body** conveying formal demonstration of its competence to carry out specific **conformity assessment** tasks	ISO/IEC 17000
certification	third-party **attestation** related to products, processes, systems or persons	ISO/IEC 17000
evaluation	combination of the **selection and determination functions** of **conformity assessment** activities	ISO/IEC 17000
selection and determination functions:		ISO/IEC 17000
sampling	provision of a sample of the object of conformity assessment, according to a procedure	ISO/IEC 17000
testing	determination of one or more characteristics of an object of conformity assessment, according to a procedure	ISO/IEC 17000
inspection	examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements	ISO/IEC 17000
review	verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfillment of specified requirements by an object of conformity assessment	ISO/IEC 17000

Table 2: Attestation concept application in the general normative context

It should be emphasized that within the general normative context the attestation adds a mark of certification (certificate or statement of conformity) to show that a given product or service is conformant after performing assessment operations. Further, it is worth to know that the general normative context does not identify which select and demonstrable function is assigned to a particular conformity assessment body. This has to be defined in a particular certification (conformity assessment) scheme.

2.3 Legal context

The legal context of conformity assessment appears from terms whose definitions are taken from the Regulation 765/2008 (see Table 3). The Regulation introduces strict organization of the market surveillance by using accreditation mechanisms for conformity assessment bodies. Only one accreditation body per Member State is allowed. Conceptually, the legal context does not disturb the general normative one.

TERM	DEFINITION
concept:	
conformity assessment	process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled
entities:	
national accreditation body	sole body in a Member State that performs **accreditation** with authority derived from the State
conformity assessment body	body that performs **conformity assessment** activities including calibration, testing, certification and inspection
activities:	
accreditation	attestation by a **national accreditation body** that a **conformity assessment body** meets the requirements set by harmonized standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific **conformity assessment** activity
peer evaluation	process for the assessment of a **national accreditation body** by other **national accreditation bodies**, carried out in accordance with the requirements (EC) No 765/2008, and, where applicable, additional sectoral technical specifications

Table 3: Terms of definitions establishing the legal context according to Regulation 765/2008

Please refer to chapter 3 for a more detailed overview of the legal context according to Regulation 765/2008.

2.4 Specific normative context

A specific normative context is established by adopting terms and their definitions from the Common Criteria standards[4]. First, the general normative context is narrowed by introducing specific types of objects to the conformity assessment performance i.e. TOE (Target of Evaluation), Protection Profile (Protection Profile), and ST (Security Target). Secondly, 'conformity assessment' is expressed as 'evaluation'. Finally, the standards define a specific framework under which all activities related to evaluation are performed, and impose specific requirements on organizations involved with regard to their activities.

[4] Currently, the whole series of ISO/IEC 15408 and ISO/IEC 18045 are subject to revision process. All terms and definitions are from official published editions dated to 2009

A systematic approach to relevant terms and definitions is presented in Table 4.

TERM	DEFINITION	SOURCE
concept:		
evaluate	assessment of a PP, an ST or a TOE, against defined criteria	ISO/IEC 15408-1
subject of evaluation:		
Target of Evaluation (TOE)		ISO/IEC 15408-1
Protection Profile (PP)	implementation-independent statement of security needs for a TOE type	ISO/IEC 15408-1
Security Target (ST)	implementation-dependent statement of security needs for a specific identified TOE	ISO/IEC 15408-1
organization:		
evaluation authority	body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements ISO/IEC 15408 for that community by means of an **evaluation scheme**	ISO/IEC 15408-1
evaluation scheme	administrative and regulatory framework under which ISO/IEC 15408 is applied by an **evaluation authority** within a specific community	ISO/IEC 15408-1
laboratory[5]	organization with a management system providing **evaluation and or testing work** in accordance with a defined set of policies and procedures and utilizing a defined methodology for **testing or evaluating** the security functionality of IT products Note 1 to entry: These organizations are often given alternative names by various approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).	ISO/IEC 19896-1
evaluation technical report	report that documents the overall verdict and its justification, produced by the evaluator and submitted to an **evaluation authority**	ISO/IEC TR 18045
activities:		
check	generate a **verdict by** a simple comparison NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.	ISO/IEC TR 18045
confirm	declare that something has been reviewed in detail with an independent determination of sufficiency	ISO/IEC 15408-1

[5] The term 'laboratory' does not appear in officially published version of Common Criteria standards, however it is introduced in a standard ISO/IEC FDIS 19896-1, and has been incorporated into revised ISO/IEC 15408-1 (currently under development)

demonstrate	provide a conclusion gained by an analysis which is less rigorous than a "proof"	ISO/IEC 15408-1
determine	affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion	ISO/IEC 15408-1
prove	show correspondence by formal analysis in its mathematical sense	ISO/IEC 15408-1
verify	rigorously review in detail with an independent determination of sufficiency Note 1 to entry: Also see "confirm". This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.	ISO/IEC 15408-1

Table 4: Specific normative concept of conformity assessment based on the Common Criteria approach

It should be noted that activities related to evaluation are expressed in different terms and meanings than selecting and demonstrating functions to be performed with regard to conformity assessment, as described in ISO 17000.

2.5 Arranged context

This context for conformity assessment of IT products security is given by international arrangements such as the Common Criteria Recognition Arrangement (CCRA)[6] – world-wide, gathering organizations from several countries, and Senior Officer Group Information Security Mutual Recognition Arrangement (SOGIS MRA)[7] – gathering organizations from the EU plus Norway. As these two arrangements both implement the same certification and evaluation framework based on the Common Criteria, the context will be described further using the SOGIS MRA documents, as relevant to European Certification Framework.

The arranged context is presented in the following table:

TERMS	DEFINITION
concept:	
evaluation:	**assessment** of an IT product or a protection profile against the IT security evaluation criteria and IT security evaluation methods to determine whether or not the claims made are justified
certification:	process carried out by a CB leading to the issuing of a certificate
organization:	
participant	A signatory to this Agreement.
accreditation body	independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the requirements of the standard

[6] https://www.commoncriteriaportal.org/ccra/
[7] https://www.sogis.org/

certification body (CB)	organization responsible for carrying out certification and for overseeing the day-to-day operation of an **evaluation and certification scheme**
evaluation facility	organization which carries out **evaluations**, independently of the developers of the IT products or protection profiles evaluated
IT Security Evaluation Facility (ITSEF)	accredited Evaluation Facility, **licensed** or approved to perform **evaluations** within the context of a particular **IT Security Evaluation and Certification Scheme**
evaluation and certification scheme	systematic organization of the functions of evaluation and certification under the **authority CB** in order to ensure that high standards of competence and impartiality are maintained and consistency is achieved
relationships imposed by the arrangement:	
accredited	formally confirmed by an **accreditation body** as meeting a predetermined standard of impartiality and general technical, methodological and procedural competence
licensed	assessed by a CB as technically competent in the specific IT technical domain and field of security evaluation and formally authorized to carry out **evaluation**s within the context of a particular within the context of a particular evaluation and certification scheme
conformant certificate	public document issued by a **compliant CB** and authorized by a **Participant** which confirms that a specific IT product or protection profile has successfully completed **evaluation** by an ITSEF
monitoring of evaluation	procedure by which representatives of a CB observe evaluations in progress or review completed evaluations in order to satisfy themselves that an ITSEF is carrying out its functions in a proper and professional manner.
voluntarily periodic assessment	**assessment of compliant CBs** (term not defined although described in the arrangement)

Table 5: Concept of evaluation and certification based on provisions of the SOGIS MRA

2.6 Comparison of terms use in different contexts

2.6.1 Equivalents

Part of fundamental terms or group of terms represent the same concept and share the same meaning regardless of the context they function in. These terms are presented in Table 1.

GENERAL NORMATIVE	LEGAL	SPECIFIC NORMATIVE	ARRANGED
conformity assessment	conformity assessment	evaluation	evaluation
certification	no equivalent	no equivalent	certification
accreditation	accreditation	not applicable	accreditation
accreditation body	national accreditation body	not applicable	accreditation body
certification body	conformity assessment body	evaluation authority	certification body (CB)

Table 6: Equivalent terms

2.6.2 Similarities

Several terms have similar meanings and could replace each other while mentioning or remembering their specific context. These terms are summarized in Table 7.

GENERAL NORMATIVE	LEGAL	SPECIFIC NORMATIVE	ARRANGED
conformity assessment scheme certification scheme	no equivalent	evaluation scheme	evaluation and certification scheme
laboratory	conformity assessment body	laboratory	IT Security evaluation facility (ITSEF)[8]
agreement group	no equivalent	not applicable	participants of the arrangement
attestation	no equivalent	no equivalent	accredited certified licensed conformant certificate
peer assessment	no equivalent	no equivalent	voluntarily periodic assessment

Table 7: Terms with similar meanings

2.6.3 Differences

Some of the terms have different meanings. Other terms should mean the same but they have significantly different definitions. Terms presented in Table 8 should be used with care, always adding the context or explanation.

GENERAL NORMATIVE	LEGAL	SPECIFIC NORMATIVE	ARRANGED
peer assessment - used in general context of conformity assessment	peer evaluation -used in relation to national accreditation bodies	not applicable	voluntarily periodic assessment - used in relation to CBs
conformity assessment activities - selection and determination functions: sampling, testing, inspection, review	no equivalent	evaluation activities: check, confirm, demonstrate, determine, prove, verify	follows 'Specific normative'

Table 8: Differences in terms

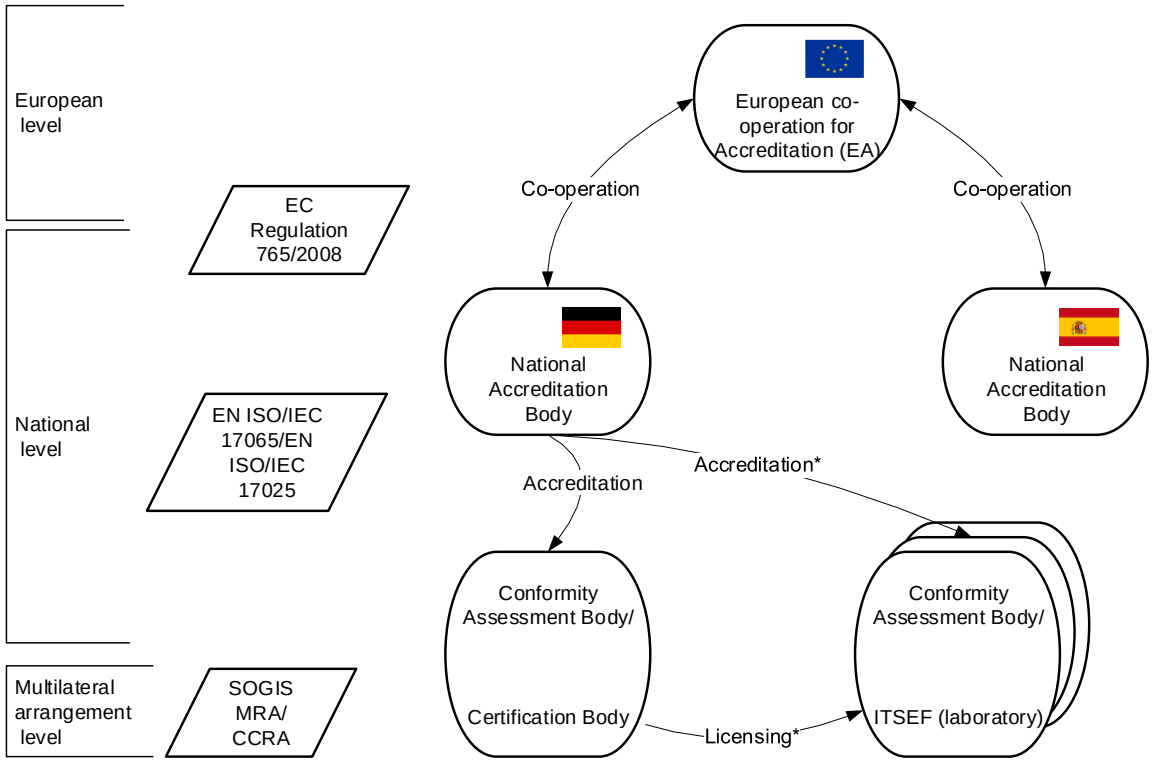
[8] A requirement for a licencing is significant attribute comparing to a general definition of laboratory. Additionally, considering differences in descriptions of evaluation activities vs. selection and determining function performance similarity criterion applies only to ITSEF which is defined by an accreditation requirement, not to an evaluation facility itself

3. Legal framework and regulations for evaluation laboratories

The legal framework in the context of the certification of products can be seen on different levels as follows:

1. General requirements as set up by the Regulation (EC) No 765/2008 of the European Parliament,
2. National level requirements from relevant accreditation bodies,
3. Certification or evaluation requirements from various standards,
4. Requirements resulting from international arrangements.

More details on these levels will be described in the following subchapters. The complete overview is summarized in the following figures:



*in some schemes licensing can be done in parallel with accreditation or as a part of accreditation

Figure 1: Overview of requirements

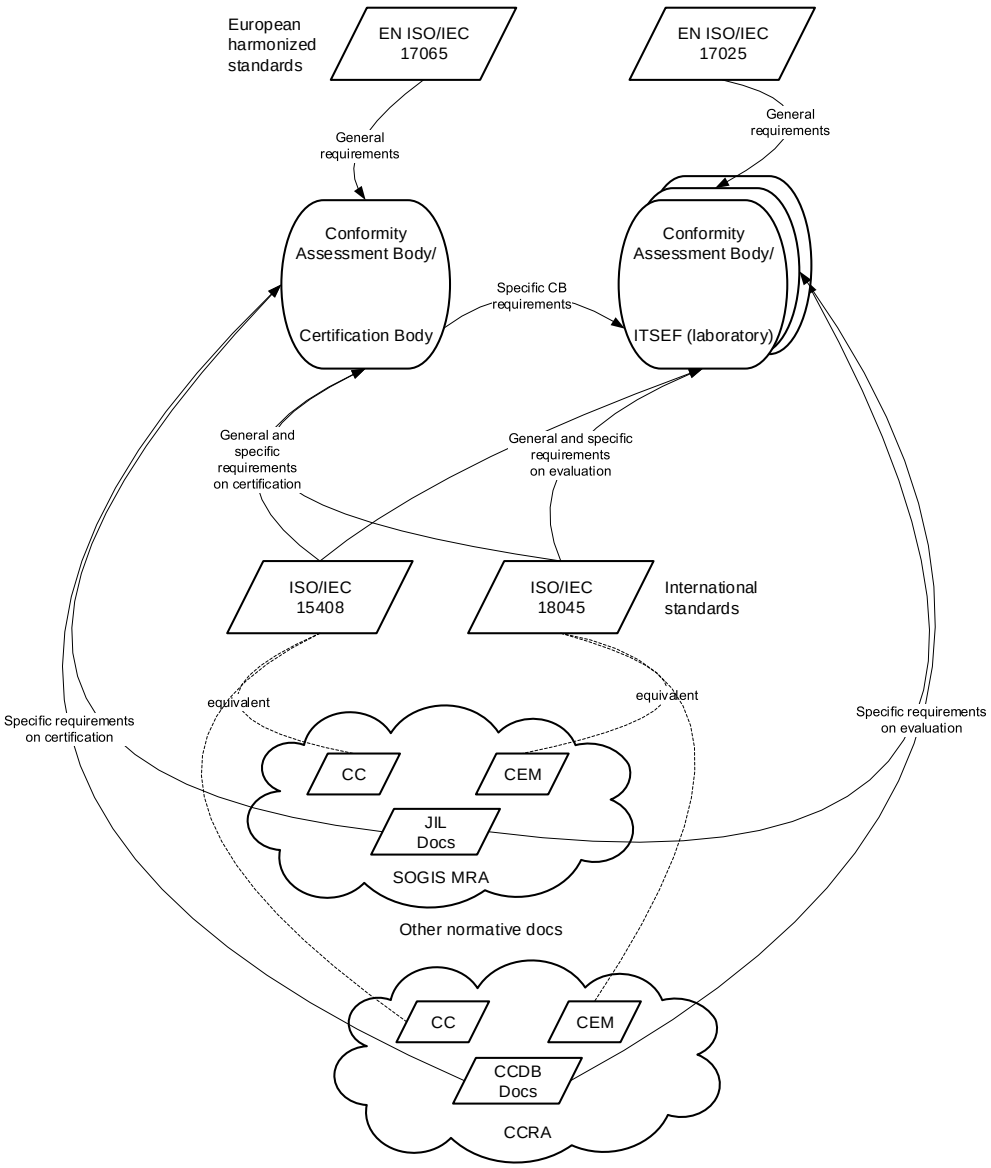


Figure 2: Sources of requirements for laboratories and Certification Bodies

3.1 Regulation No 765/2008

With Regulation (EC) No 765/2008 the EU set requirements related to the accreditation of bodies who perform conformity assessments for products. This regulation applies to European national accreditation bodies that in turn perform the accreditation of the evaluation laboratories.

It is an essential part of this regulation that each Member State of the European Union shall appoint a single national accreditation body. (Article 4, 1).

This national accreditation body shall, when requested by a conformity assessment body, determine whether that conformity assessment body is competent to carry out a specific conformity assessment activity. Where it is found to be competent, the national accreditation body shall issue an accreditation attestation to that effect. This way, a harmonized European structure for the accreditation of laboratories is built.

On the European level, one body has been recognized as the *European Body for Accreditation*. This body is the European co-operation for Accreditation or EA. EA is an association of national accreditation bodies in Europe that are officially recognised by their national governments to assess and verify—against international standards—organisations that carry out conformity assessment services such as certification, verification, inspection, testing and calibration.

For the use in this report, EA has the following roles:

- EA cooperates with the European Commission in questions of accreditation,
- EA shall allow national accreditation bodies within the Members States to become a member of EA, provided that they comply with the rules of EA,
- EA shall provide its members with peer evaluation services.

In the context of this report, the peer evaluation services of this body are of specific importance.

'peer evaluation' refers to a process for the assessment of a national accreditation body by other national accreditation bodies, carried out in accordance with the requirements (EC) No 765/2008, and, where applicable, additional sectoral technical specifications;

Each member of EA (i.e. each European Accreditation body) agrees to take part in the process of peer evaluation, both actively and passively in order to ensure that all members of EA follow the corresponding regulations. By the use of the peer evaluation procedures, a consistent quality should be guaranteed throughout the complete system.

3.2 National level

When the scope of our view changes to the national level, [ISO17025] and [ISO17065] are the most relevant standards after which each of the national accreditation bodies will perform the accreditation of the conformity assessment bodies. Further, from the laboratories perspective, [17027] is of the utmost interest.

[ISO17025] defines general requirements on competency that will have to be met by the laboratory providing testing (including evaluation), or calibration services. It specifically poses requirements on:

- General Management Requirements
  - Control of Documents
  - Subcontracting, purchasing and service to the customer (including complaints)
  - Control of nonconformity testing and/or calibration work
  - Improvements, Corrective Actions, internal audits and reviews
- Technical Requirements
  - General requirements
  - Accommodation and environmental conditions
  - Test and calibration methods
  - Equipment
  - Measurement traceability
  - Handling of test and calibration items
  - Assuring the quality of test and calibration results
  - Requirements on reporting the results

A new edition of [ISO17025] is being elaborated at the time of writing of this report. Among new features, it will offer a process oriented approach, which constitutes new value and significant changes in accreditation schemes.

Even though it is not a strict requirement, evaluation laboratories in the area of IT-security often also maintain a quality management system in accordance with [ISO9000] and an information security management system in accordance with [ISO27000].

[ISO17065] defines the requirements that will have to be met by the certification authority. It specifically poses requirements on:

- General Requirements
  - Legal requirements
  - Impartiality
  - Liability and financing
  - Non-discriminatory conditions
  - Confidentiality
  - Publicly available information
- Structural Requirements
  - Organization Structure
  - Mechanisms for safeguarding impartiality
- Resource Requirements
  - Personnel
  - Ressources for evaluation
- Process Requirements
  - Applications and Application Review
  - Evaluation and Review
  - Certification decision and documentation
  - Directory of certified products
  - Surveillance
  - Changes affecting certification
  - Termination, reduction, suspension or withdrawal of certification
  - Records
  - Complaints
- Management System Requirements
  - Options
  - General management system documentation
  - Control of documents and records
  - Management review
  - Internal audits
  - Corrective actions
  - Preventive actions

3.3 Standard Level

Below the level of [ISO17025] and a potentially implemented management system, the view will change to the standards according to which a conformity assessment body (i.e. the actual evaluation laboratory) performs its assessments.

Prominent examples include the Common Criteria (aka ISO/IEC 15408 ([ISO15408] and ISO/IEC 18045 [18045][9]) and [ISO19790][10]

Beside their technical criteria for conformity assessment, these standards bring further organizational requirements.

As an example, this can be analyzed for the Common Criteria (CC):

3.4 Requirements from international arrangements

The CC distinguishes between the processes of evaluation and certification. The evaluation is the process that can be seen as the assessment of a product (the so-called Target of Evaluation) against defined requirements.

The certification process oversees the evaluation and ends with the actual certificate. CC requires that the certification process is performed by a party independent from the evaluation laboratory.

3.4.1 General considerations

The international recognition of certifications that are performed according to Common Criteria is one of the major advantages and benefits of using Common Criteria as reference standards. However, from the perspective of an evaluation laboratory, this advantage also goes along with an additional set of requirements that have to be met. The following two subchapters introduce the major areas from which these requirements arise, namely the CCRA and the SOG-IS agreement.

3.4.2 CCRA

The arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security ([CCRA]) is the first agreement on the international recognition of certificates issued on conformity assessment against Common Criteria.

The purpose of this Arrangement is to ensure that evaluations are performed based on consistent standards and with a high level of assurance, to improve the availability of evaluated products and Protection Profiles, to eliminate the burden of redundant evaluations and to continuously improve the efficiency and cost-effectiveness of evaluations.

The primary goal of the arrangement is to ensure that IT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for further evaluations.

A Management Committee, composed of senior representatives from each signatory's country of the CCRA, has been established to implement the Arrangement and to provide guidance to the respective national schemes conducting evaluation and validation activities.

[9] Basically, Common Criteria consist of: 1) 3-part standard containing: concepts and models (ISO/IEC 15408- 1), security functional requirements (ISO/IEC 15408 2), security assurance requirements (ISO/IEC 15408-3) and 1-part standard containing evaluation methodology description (ISO/IEC 18045 "Common Methodology for Information Technology Security Evaluation" (CEM)). Further details are provided in Chapter 5.

[10] ISO/IEC 19790 deals with Security requirements for cryptographic modules. It is the ISO pendant of the FIPS 140-2 requirements.

The requirements of the Common Criteria are mainly developed by an international consortium known as Common Criteria Development Board (CCDB) and Common Criteria Maintenance Board (CCMB). Usually, members of these consortia have a governmental background.

CCDB manages the technical work program for the maintenance and ongoing development of the CC and CEM and reach agreement on the application of the CC and CEM to evaluations being carried out by the CCRA certificate producing nations to ensure harmonization across qualifying nations. The principal purpose of CCMB is to process requests for inclusion of Change Proposals (CP), based upon national CC and CEM development requirements and taking into account CCRA requirements as specified by the CCDB.

For an evaluation laboratory, the work of the CCDB goes along with a set of requirements for the daily work. Beside the criteria that are laid down in CC and a set of supporting documents that are developed and maintained by the CCDB, the certification body of each member of the CCRA is responsible for oversight of the compliance of the evaluation laboratory with the criteria.

3.4.3 SOG-IS

Beside the arrangement laid down in the CCRA, an additional recognition agreement exists on the European Level.

The SOG-IS (Senior Officers Group) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

The participants of the SOG-IS agreement have a slightly different perspective than the participants of the CCRA. SOG-IS mainly focusses on coordinating evaluation activities around Common Criteria among European Certification Bodies (also to gain a strong standing within CCRA) and to coordinate the development of Protection Profiles. It should be noted that the SOGIS MRA scope of interest is limited to two technical domains of IT products i.e. “Hardware devices with security boxes CC” and “Smartcards and similar devices CC”.

However, the SOG-IS agreement also comprises a recognition of Common Criteria certificates among the participants of the agreement. In contrast to the CCRA, two things are important to mention about the recognition that are regulated under this agreement:

1) The recognition of certificates covers all evaluation assurance levels up to EAL7 (compared to only EAL2 typically under the CCRA)
2) The recognition above EAL 4 is only covered for defined technical areas when schemes have been approved by the management committee for this level.

Similar to CCRA, the arrangement provides for member nations to participate as certificate consuming participants or as certificate producers.

The original arrangement signed in 1997 (updated to incorporate the use of Common Criteria in 1999) was updated in 2010 for two reasons; firstly, to provide a robust mechanism allowing new schemes to take part as certificate producers and, secondly, to limit the higher levels of recognition to agreed technical domains where adequate agreement around evaluation methodology, laboratory requirements, attack methods etc. are in place.

In order to achieve the higher level of recognition under the SOG-IS agreement, it has been necessary to develop and publish a set of supporting documents that have been developed by different working groups

in the context of the SOG-IS agreement. These documents build up the Joint Interpretation Library (aka JIL documents) and comprise mandatory documents that have to be followed during each evaluation of a product that falls into a technical domain covered by the SOG-IS agreement and guidance documents that are optional regarding their use. More details will be given in Chapter 5.

The certification bodies which are part of the arrangement ensure that all evaluation bodies will follow those criteria in addition to the criteria that has been published by the CCMD/CCDB under the CCRA.

4. Organisation of laboratories

4.1 Legal forms of laboratories

4.1.1 Introduction

In general, laboratories operate under respective national schemes (see 4.2). Although all are providing services of evaluating the security of ICT products based on an approved and unified methodology, their legal and business context varies, reflecting characteristics of local economies and policies of the Certification Body. By researching all licensed laboratories world-wide this report will try to identify relevant patterns, similarities and differences. The research will focus on the important implication from the European Union's perspective. Respective European schemes are indicated in pink in every table.

4.1.2 Research methodology

Presented information has been gathered by means of Internet based research.

For all licensed laboratories the type of legal entity has been determined, using the respective country's business register. The following types have been identified:

- Private company – independent legal entity, usually similar in form to a limited liability corporation,
- Traded private company – independent legal entity, traded on a local stock exchange,
- Research institute – non-profit entities, set up by industry members or universities, and
- Government agency – laboratories which are part of the country's government.

By investigating companies' websites the importance of the Common Criteria evaluations (and ICT certification more broadly) for their business model has been qualified, estimating them on a range from core to minimal, with labels "IT Security oriented" and "certification oriented" signaling states in between. The assessment is subjective.

4.1.3 Presentation of results

4.1.3.1 Laboratories in numbers

All laboratories listed as being currently in operation within the CCRA framework[11] were the subject of analysis. It should be emphasized that laboratories operating in the context of the SOGIS Mutual Recognition Arrangement[12] are a subset of the analyzed set of laboratories.

Major findings with regard to licensed laboratories are presented below.

This report analyzes 67 laboratories licensed under 16 operating schemes. As some laboratories are providing evaluation services under more than one national scheme (see below) a total of 60 separate entities has been counted in total.

The number of licensed laboratories operating under respective scheme range from 1 (India) to 9 (USA).

[11] https://www.commoncriteriaportal.org/labs/
[12] https://www.sogis.org/uk/status_participant_en.html

less than 3	6	Australia, India, Malaysia, the Netherlands, Sweden, UK
3-5	5	Canada, Japan, Norway, Spain, Turkey
6 and more	5	France, Germany, Italy, Korea, US

Table 9: Number of licensed laboratories under different schemes

37 laboratories fall under the category of '(traded) private company' which is more than 50% of all licensed laboratories. In the context of this study they are called 'legally independent'. Legally independent laboratories constitute a majority of licensed laboratories in Norway (100%), Germany (87%) and France (60%).

The second group of security evaluation providers consists of laboratories operating as parts of multinational companies with a wide portfolio of ICT products and services. They constitute a majority of licensed labs in Australia (100%), UK (100%) and Canada (75%).

The third group includes research institutes (both industry funded and affiliated with universities) and government agencies. There are several cases that highlight their importance. A governmental agency is the only licensed laboratory under the Indian scheme. Research institutes constitute a significant proportion of licensed labs in Japan and Korea.

All discussed figures are presented in Table 10.

COUNTRY	NUMBER OF LICENSED LABS	PRIVATE COMPANY	TRADED PRIVATE COMPANY	PART OF A MULTINATIONAL CORPORATION	RESEARCH INSTITUTE	GOVERNMENT AGENCY
Australia	**2**			2		
Canada	**4**	1		3		
France	**6**	4		1	1	
Germany	**8**	7			1	
India	**1**					1
Italy	**6**	3	2	1		
Japan	**5**	1		1	3	
Korea	**6**	2			2	2
Malaysia	**2**			1		1
Netherlands	**2**	2				
Norway	**4**	4				
Spain	**3**	1	1			1
Sweden	**2**	2				
Turkey	**5**	1	1	2		1
UK	**2**			2		
USA	**9**	5		4		
Total	**67**	33	4	17	7	6

Table 10: Licensed laboratories operating under CCRA SOGIS schemes - legal forms

Several schemes allow laboratories based abroad to be licensed. Table 11 provides the list:

NAME	COUNTRY OF ORIGIN	SCHEME(S)
atsec Germany	Germany	Germany, Italy
Systems Software Laboratory CCLAB	Hungary	Italy
Brightsight	the Netherlands	the Netherlands, Japan, Norway, Turkey
TUV GmbH Evaluation Body for IT Sec	Germany	Germany, Japan
Advance Data Security	USA	Norway
Epoche and Espri	Spain	Spain, Turkey
CygnaCom Solutions	USA	USA, Turkey

Table 11: Country of origin and scheme assignment for laboratories

It should be noted that all licensed laboratories in following schemes: Italy, Japan, Norway and Turkey are providing evaluation services from abroad (they do not have locally based entities operating under the scheme).

4.1.3.2 Common Criteria evaluation as a business

- Further analysis comes to business perspective of laboratories. Considering the following classification:
  - Core: Common Criteria evaluations is the core business of the entity; additionally, the security certification (as in both cases of importance) focus also falls under 'Core' label;
  - IT security oriented: the entity focuses on ICT security services, however, Common Criteria evaluations play important role in their portfolio;
  - Certification oriented: the entity provides wide range of evaluation and certification services in many fields;
  - Minimal: CC evaluations are only a small part of a wide portfolio of products and services, including providing integrated IT or IT security solutions.

We have quantified laboratories per business type, with regards to all analyzed schemes (see Table 12).

COUNTRY	TYPE OF BUSINESS				
	core	certification oriented	IT security oriented	minimal	Total
Australia				2	**2**
Canada			1	3	**4**
France			3	3	**6**
Germany	3		3	2	**8**
India	1				**1**
Italy	3	1		2	**6**
Japan	3		1	1	**5**
Korea	5	1			**6**
Malaysia	1			1	**2**
Netherlands	2				**2**
Norway	3			1	**4**
Spain	1	1		1	**3**
Sweden	1			1	**2**
Turkey	4			1	**5**
UK				2	**2**
USA	3			6	**9**
Total	**30**	**3**	**8**	**26**	**67**

Table 12: Type of business of laboratories per scheme

Differences between European laboratories and others with respect to type of business is discussed in next section.

4.1.4 Differences between European laboratories and others

While analyzing the legal form with regards to relevant arrangements gathering schemes significant differences can be identified.

It appears majority of licensed laboratories operating under the SOGIS scheme are independent private companies focused on evaluation services themselves, and this figure is significantly higher than for laboratories under the CCRA.

This finding is summarized in Figure and Figure 4, respectively.

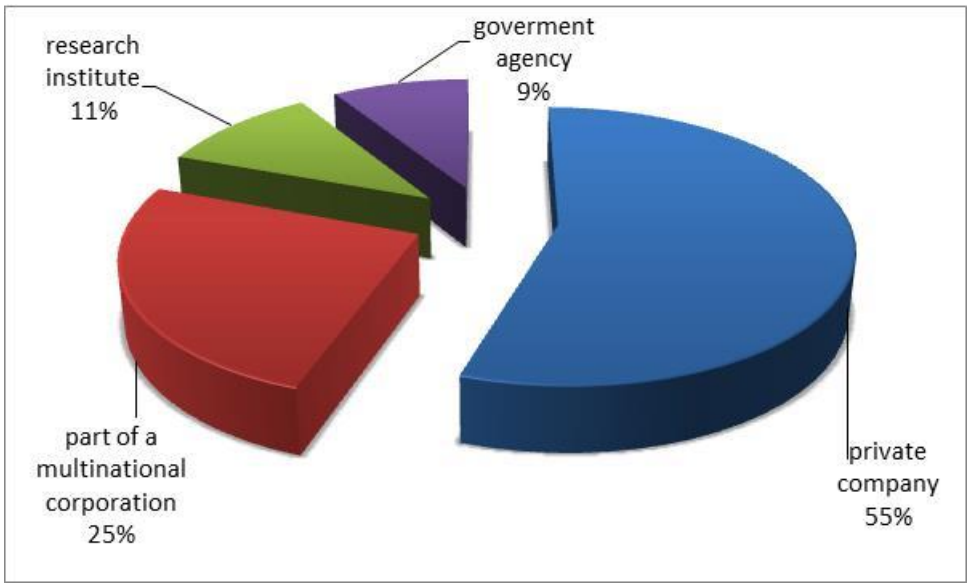


Figure 3: Licensed laboratories operating under CCRA scheme

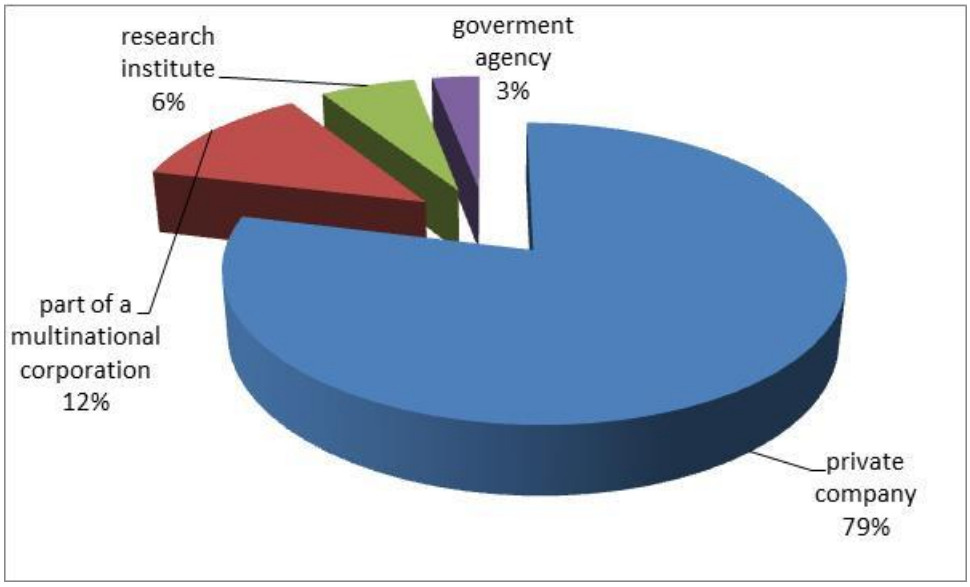


Figure 4: Licensed laboratories operating under SOGIS MRA scheme

Considering the importance of the Common Criteria evaluation from the business perspective one can compare European and non-European schemes. For this purpose, 52 individual business entities ie. local branches counted as singular, multinationals - as one instance have been identified. The results are presented in Figure 5 and Figure 6, respectively.

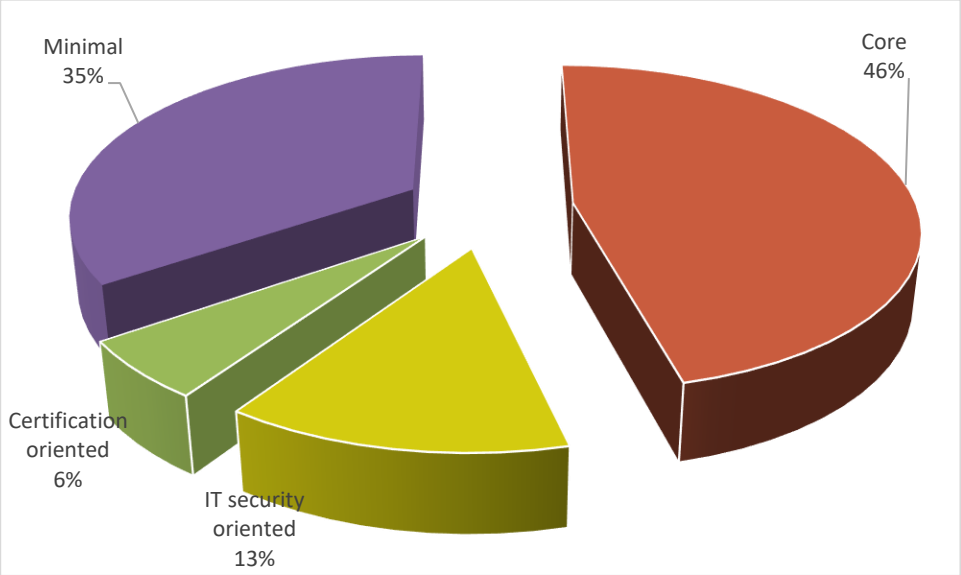


Figure 5: Importance of CC evaluation for the companies' business model under the CCRA

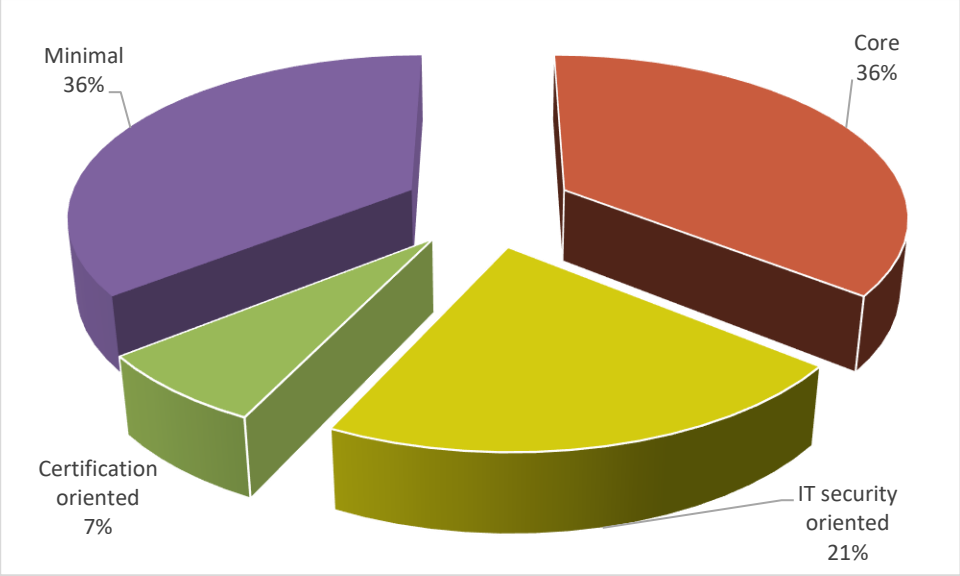


Figure 6: Importance of CC evaluation for the companies' business model under the SOGIS MRA

Worldwide, for 46% of the studied laboratories certification under CC is deemed as core business. A much smaller proportion (13%) of the laboratories focuses on IT security, of which certification is only a part. The smallest group (6%) consists of laboratories that provide certification services in many fields. The rest of the laboratories (35%) are parts of large companies, often multinational, for which CC certification is of minimal importance. Results of classification limited to the SOGIS MRA follow similar patterns, with the exception of the relative greater importance of IT security oriented business model.

4.2 Licensing and supervising

4.2.1 Introduction

For the purpose of analysing relevant characteristics, the scheme processes have been divided into two phases: licensing and then supervising. The research has been conducted with respect to all 16

certification schemes although finding a complete set of information for all these schemes has not been possible in the given timeframe.

4.2.2 Licensing

4.2.2.1 Application procedure

A licencing mechanism has been identified in all analysed schemes. The most distinguished features are:

- one- or two-step procedure: the proceeding for granting a license can be divided into two phases. In some schemes it is allowed to obtain a provisional appointment after passing technical examination of the laboratory readiness, and then a permanent license after successfully completing the test evaluation,
- technical examination of the applicant capability is sufficient, or additionally, performing a test evaluation is necessary for the applicant to get a license,
- getting an accreditation as a prerequisite: **being accredited against ISO/IEC 17025 is mandatory in all analysed schemes**, however, in some schemes currently it is allowed to start the assessment by a Certification Body without fulfilling the accreditation requirement by the applicant.

It should be noted that European schemes are licensing the laboratories under CCRA and - in parallel - under SOGIS MRA. The characteristics of the application procedure are summarized below.

		APPLICATION PROCEDURE		
No.	Country	Fulfilling technical requirements	Test evaluation performed by the applicant	Accreditation against ISO/IEC 17025 as a prerequisite
1	UK	Provisional Appointment	Permanent Appointment	no
2	Australia & New Zealand	license granted after assessment and upon a licensing agreement	not applicable	no
3	Sweden	part of the assessment procedure	license granted	no
4	Canada	part of the assessment procedure	license granted	yes
5	Germany	part of the assessment procedure	license granted	yes
6	The Netherlands	part of the assessment procedure	both, accreditation and licensing based on successful trial evaluation	no
7	USA	license granted after assessment and upon a licensing agreement	not applicable	yes
8	Malaysia	license granted after assessment	not applicable	no
9	Japan	part of the assessment procedure	license granted	yes

Table 13: Application procedure differences among schemes

4.2.2.2 Licensing fees

There is a variety of licensing fee models among schemes. Some do not apply any fee, some others have only an introductory fee (for the Application), and then for renewal of the license, and some implement subscriptions. It should be noted that fees can be applicable to accreditation, but this is out of the schemes control hence not discussed here.

All findings concerning the fee models for licensing are summarized in Table 14.

	COUNTRY	LICENSE FEES	
		Introductory fee	**Subscription or membership**
1	UK	no (see next column)	yes (applicable to Provision Applicants as well)
2	Australia & New Zealand	no	no
3	Sweden	1) Application 2) License	yes (annual)
5	Germany	Dependent on the inspection field	renewal - every 2 years
7	USA	no	no
8	Malaysia	Application	Annual subscription for 3 consecutive years) Renewal - every 3 years
9	Japan	1) Application 2) Evaluator Qualification	not identified

Table 14: Licence fee models for laboratories

4.2.2.3 Independency of evaluation

Preserving independency of evaluation is fundamental for the third-party evaluation. Schemes impose on licensed laboratories various requirements to ensure actual independency of evaluations. The great majority of commercial laboratories provides consultancy services, which pose a significant source of potential conflict of interests. Every scheme addresses the issue, some provide a time period, in which consultancy work prohibits an individual from working as an evaluator, some others set up general rules only for avoiding conflicts of interest. We have found the strongest rule in the Japanese scheme where providing consultancy services in parallel to the evaluation with regards to a given evaluated product is clearly forbidden.

A summary of requirements concerning independency is given in Table 15.

	COUNTRY	RULES FOR THE EVALUATION INDEPENDENCE
1	UK	– autonomous in operational and administrative; – evaluation independent of TOE development; – no evaluation of the work of any group or division within the parent company (the rule may be relaxed at the discretion of the CB); – consultancy can be provided unless it does not impair the independence of the evaluation i.e. an individual cannot evaluate his or her own work.
2	Australia & New Zealand	– functional separation from the lab's parent organization must be maintained; – evaluating a product of parent company or within the group is not allowed; – evaluation support consultancy and evaluation services are permitted, however the laboratory must be able to demonstrate the separation of these activities from evaluation activities.
3	Sweden	– establishing and implementing documented procedures for identifying conflicts of interest and for ensuring that such conflicts do not adversely influence the quality of the evaluations is required; – pre-evaluation consulting may be provided by the laboratory providing proper separation of evaluation and consultancy work; – personal involvement of the laboratory personnel with the supplier of a product under evaluation within the preceding two years, either in design of the product or consultancy services to the supplier regarding methods of dealing with matters that are barriers to the product being certified, is prohibited.
4	Canada	– sufficient separation of control with the parent company shall be demonstrated; procedures to ensure no conflict of interest between personnel advising and evaluating shall be established and implemented.
5	Germany	– conflict of interests with regards to the outcome of an evaluation for the laboratory , its parent corporation and individual staff members shall be identified and removed; – labs have to identify potential conflicts of interest in the beginning of an evaluation and report to the certification authority; – any person active in the evaluation process cannot have been involved in the TOE development.
6	The Netherlands	– an individual cannot be hired by the Sponsor for consultancy within 2 years of termination of their employment at the laboratory performing the evaluation.
7	USA	– conflict of interest with regards to the outcome of an evaluation for the laboratory , its parent corporation and individual staff members shall be identified and removed ; – consulting and evaluation activities shall be separated within the laboratory (ie. different people shall be assigned to the two).
8	Malaysia	– any person active in the evaluation process cannot have been involved in the TOE development, consultancy to the Sponsor within the last 2 years.
9	Japan	– laboratories are prohibited from providing consulting services in parallel to evaluation one with regards to a given evaluation; – in case of divisions of larger companies labs have to be operational independent, and operating on own budget.

Table 15: Independency requirements

4.2.3 Supervision

4.2.3.1 Supervising the evaluations

In general, certification bodies are obliged to oversee the evaluation process as they are held responsible for issued certificates. General provisions on the supervision activities can be found in relevant documentation of every scheme. However, schemes differ significantly if it comes to details. In some schemes dedicated certifiers actively participate in the evaluation, in others a lead certifier even validates every part of the evaluation process, while in some others the nominated certifier plays a passive role, and only approves the final Evaluation Technical Report. Various approaches depending on the perceived complexity of evaluation can be applied as well (for example, see the Spanish scheme characteristics).

The summary of findings is presented in Table 16.

	COUNTRY	CB'S ROLE IN THE EVALUATION PROCESS
1	UK	– determining whether a TOE will be certifiable in principle; – monitoring all evaluations conducted under the Scheme; – assessing all evaluations' results and issuing certificates; – (optionally) conducting Evaluation Progress Reviews.
2	Australia & New Zealand	– accepting evaluation tasks and plans to conduct evaluation; – allocating two certifiers allocated to an evaluation task (certifiers conduct oversight through meetings, discussing technical details, reviewing reports, maintaining certification records, monthly reports on progress); – reviewing draft Evaluation Technical Report.
3	Sweden	– deciding whether to undertake or decline the Certification; – evaluating partially the result by single evaluation reports (SER), each submitted to the certifier for acceptance, and full evaluation report acceptance; – creating technical oversight reports; – possible direct supervising the Developer Sites or evaluator's independent testing by evaluator.
4	Canada	– determining whether the Target of Evaluation is suitable for evaluation; – providing technical oversight (allocated personnel, i.e. independently performing a subset of evaluation activities and comparing the results, directly observing activities in progress, reviewing reports); – accepting Evaluation Technical Report (ETR).
5	Germany	– determining whether a TOE will be certifiable in principle; – oversighting the process; – monitoring certain activities of the evaluation facility, such as the execution of tests/penetration tests or the execution of site audits at the developer in each case on site, – partial reports are only "reviewed and commented on" only final ETR is subject to approval.
6	The Netherlands	– accepting applications for certificates; – supervising every evaluation (by appointing Certifier who accepts reports and creates Certification Report); – executing the evaluator obligations to submit monthly status reports.

7	USA	– implementing active involvement in the evaluation process: – government evaluators may be assigned as members of a laboratory evaluation team; – each evaluation gets a Validator, as a liaison between certification body and a laboratory (they decide what is the scope of their involvement), mostly for technical oversight; observation reports; – Technical Rapid Response Team is assigned for each technology type and is expected to provide timely response to questions; – Evaluation Consistency Review is to ensure the LT technical consistency, in conjunction with TRRT addresses issues across multiple evaluations
8	Malaysia	– accepting the evaluation; – supervising (at least 2 certifiers assigned) the evaluations by: – technical review of evaluators' work at predefined key points in the evaluation; monthly progress reports; – review and approve test plans; – prepare certification report.
9	Japan	– accepting the evaluation; – agreeing on evaluation work plan.
10	Norway	– implementing oversight activities: as part of inspections may be in place, certifiers may be present during testing; – approving the ETR.
11	Spain	– introducing 3 levels of monitoring of an evaluation: – basic level (low complexity, not long, only ETR required), – medium level (default: partial reports corresponding to the evaluation activities, which in turn correspond with the evaluation of the security assurance requirement classes in the standard), – monitoring level (exceptionally to evaluations having a larger than normal number of nonconformities, special technological challenges - at discretion of the CB).
12	France	– oversighting the process; – approving the ETR.

Table 16: Supervising the evaluation in relevant schemes

4.2.3.2 Auditing or monitoring

Schemes vary in their understanding of auditing or monitoring with respect to licensed laboratories. Such activities are part of continuous supervision of the laboratories. However, the approach, depth and frequency of such activities show different ways of achieving the objective. Some schemes include a procedure for monitoring the laboratory operations upon defining trigger criteria, others rely on periodic technical assessments, and some others on analysing periodic reports submitted by the laboratory.

The findings are presented in Table 17.

	COUNTRY	AUDIT OR MONITORING PROCEDURE
1	UK	– monitoring the performance of a laboratory can be activated at any point during the laboratory membership of the scheme; – as a minimum: annual audit to co-incide with a laboratory annual contract extension (in case, an existing laboratory wishes to extend their scope of operation).
2	Australia & New Zealand	– obligatory reporting to the CB of future evaluation tasks, changes to staff every 3 months.
3	Sweden	– yearly assessment resulting in automatically renewal of the license; surveillance of the laboratory operation by continuous certification oversight.
4	Canada	– Observation Reports generated in response to issues that require corrective action by the laboratory; – assessment of personal changes.
5	Germany	– annual audits
6	The Netherlands	– submitting a list of the qualified evaluators with proofs of competence on annual base is required; – annual formal technical assessment of the laboratory.
7	USA	– new audit process "Check-In/Check-Out" is currently being implemented*
8	Malaysia	– submitting an annual business report with key performance measures: time to complete; effort spent; vulnerabilities discovered; consumer satisfaction etc; – reviewing of the laboratory operations at the discretion of CB.
9	Japan	– periodic assessments by the CB (not if lab is periodically assessed by the Japanese Accreditation Body).
10	France	– licensing audit performed every 2 years; – checking e if the laboratory meets the licensing criteria - at any time.

*CB conducts periodic meetings in which those involved in the evaluation process will track progress and discuss issued within a specific evaluation

Table 17: Auditing or monitoring the licensed laboratories

5. Standards used in the evaluation process

5.1 Assurance paradigm in ISO/IEC 15408-3

The main use of ISO/IEC 15408 is to assess the security of IT products. However, every IT product may be used in many ways, and in many types of environment, so the notion of security can vary with context. That means that the result of an ISO/IEC 15408 evaluation is never “this IT product is secure”, but is always “this IT product meets this security specification”. In other words, security evaluation is a process of determining and then proving - with sufficient level of assurance – that the IT product is conformant (or not) to defined criteria.

As ISO/IEC 15408-3 states, assurance is gained by active investigation performed by an evaluator. This includes the use of various techniques like:

- analysis and checking of process(es) and procedure(s);
- checking that process(es) and procedure(s) are being applied;
- analysis of the correspondence between TOE design representations;
- analysis of the TOE design representation against the requirements;
- verification of proofs;
- analysis of guidance documents;
- analysis of functional tests developed and the results provided;
- independent functional testing;
- analysis for vulnerabilities (including flaw hypothesis);
- penetration testing (i.e. finding and exploring vulnerabilities).

The ISO/IEC 15408 philosophy asserts that greater assurance results from the application of greater evaluation effort. This increasing level of effort is based upon:

1. scope -- that is, the effort is greater because a larger portion of the IT product is included;
2. depth -- that is, the effort is greater because it is deployed to a finer level of design and implementation detail;
3. rigour -- that is, the effort is greater because it is applied in a more structured, formal manner.

To structure all assurance requirements of every IT product subject to evaluation is described in formal language of assurance classes, families and components.

It is beyond the scope of this paper to describe all assurance elements presented in ISO/IEC 15408-3 in detail, but one should notice the least grained element i.e. assurance component - relevant to the IT product - includes all information needed to perform an evaluation in the scope of such element:

a) Dependencies with other assurance components, either from the same family/class, or different one;

b) Developer action elements: i.e. set of actions is further qualified by evidential material referenced in the following set of elements.

c) Content and presentation of evidence elements: i.e. the evidence required, what the evidence shall demonstrate, and what information the evidence shall convey.

d) Evaluator action elements: i.e. a set of actions that explicitly includes confirmation that the requirements prescribed in the content and presentation of evidence elements have been met. It also includes explicit actions and analysis that shall be performed in addition to that already performed by the developer. Implicit evaluator actions are also to be performed as a result of developer action elements which are not covered by content and presentation of evidence requirements.

An example of the assurance component and related actions on the evidence submitted is presented in Table 18.

Assurance element	Code	Description
Class:	AVA	Vulnerability Assessment
Family:	AVA_VAN	Vulnerability Analysis
Component:	AVA_VAN.1	Vulnerability Survey
Dependencies	ADV_FSP.1	Basic functional specification
	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Developer action elements:	AVA_VAN.1.1D	The developer shall provide the TOE for testing
Content and presentation elements:	AVA_VAN.1.1C	The TOE shall be suitable for testing
Evaluator action elements:	AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
	AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Table 18: AVA_VAN.1 assurance component presentation

The overall assurance of a given evaluation is expressed then by including building blocks in the form of the relevant assurance components reflecting the scope, depth and rigour of the evaluation effort, as described above. To make comparison among evaluated products easier ISO/IEC 15408-3 comes with predefined assurance packages called 'evaluation assurance level n' (EALn), n=1,....,7. The rule for the EALn+1 is that it includes all assurance components of the EALn plus set of components representing broader scope, deeper or more rigorous approach to the evaluation than relevant components of the EALn.

5.2 Evaluation process according to ISO/IEC TR 18045

There are direct relationships between ISO/IEC 15408-3 assurance structure (i.e. class, family, component and element) and the structure of evaluation process as described in ISO/IEC TR 18045 (see Figure 7).

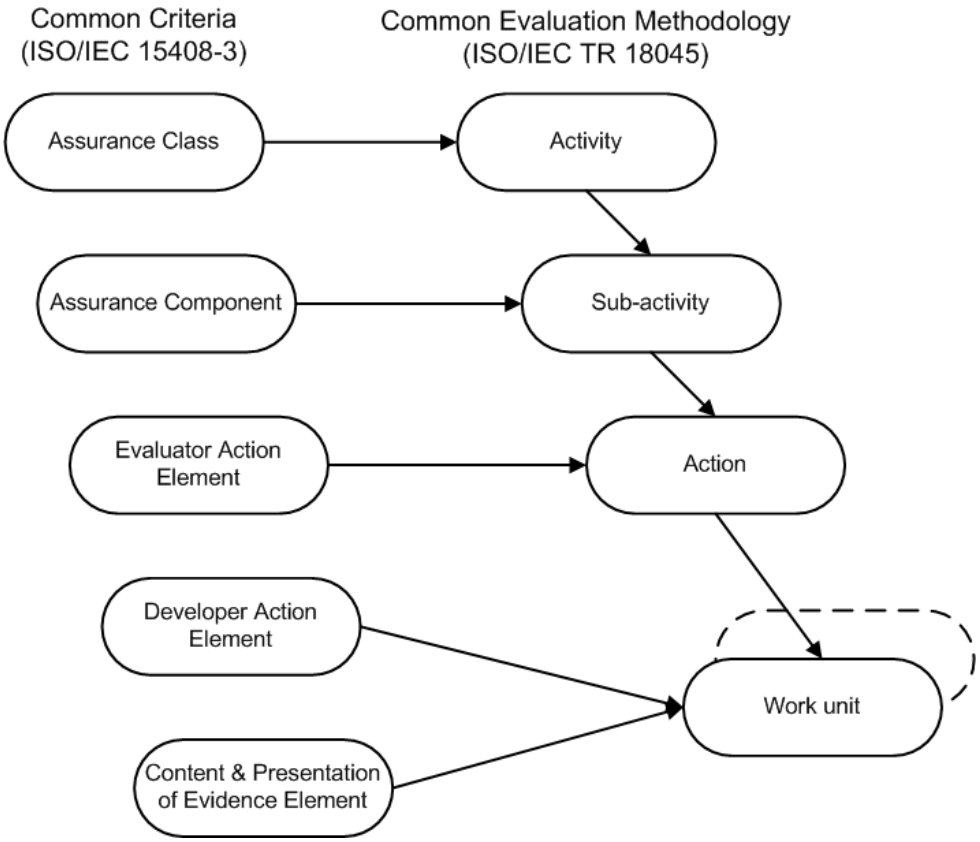


Figure 7: Structural relationships in the evaluation process (source: ISO/IEC 18045)

The ISO/IEC TR 18045 provides a description of evaluation process in terms of:

a) roles and responsibilities of the parties involved, and
b) a general evaluation model, as a direct consequence of relationships presented above.

The general model defines the following roles: sponsor, developer, evaluator and evaluation

Four distinct roles i.e. sponsor, developer, evaluator and evaluation authority[13] are involved in the evaluation process.

The **sponsor** is responsible for requesting and supporting an evaluation. This means that the sponsor establishes the different agreements for the evaluation (e.g. commissioning the evaluation). The sponsor ensures that the evaluator is provided with the evaluation evidence.

The **developer** produces the TOE and is responsible for providing the evidence required for the evaluation (e.g. training, design information), on behalf of the sponsor. One should observe that these two roles are not necessarily distinguishing each other in every evaluation. In simple instances (e.g. EAL1 evaluations) it could be one person.

The **evaluator** performs the evaluation tasks required in the context of an evaluation: the evaluator receives the evaluation evidence from the developer on behalf of the sponsor or directly from the sponsor,

[13] 'Evaluation authority' can be called 'certification body in specific contexts, see Chapter 2 for further details.

performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority.

The **evaluation authority** establishes and maintains the scheme, monitors the evaluation conducted by the evaluator, and issues certification/validation reports as well as certificates based on the evaluation results provided by the evaluator.

Each evaluation, whether of a PP (Protection Profile) or TOE (Target of Evaluation) with its ST (Security Target), follows the same **general model**, and has four evaluator tasks in common: the input task, the output task, the evaluation sub-activities, and the demonstration of the technical competence to the evaluation authority task.

The input task and the output tasks are related to management of evaluation evidence and to report generation, respectively.

Every evaluation sub-activity is performed with respect to an ISO/IEC 15408-3-mapped evaluator action element (explicit or implied) and ends with the evaluator verdict as a result of the corresponding evaluation. An initial state of the verdict is 'inconclusive', and can be changed into 'pass' or fail' after the sub-activity is completed. If all conditions for completing the evaluator action element are not fulfilled, the verdict remains as 'inconclusive'. An overall verdict is 'pass' if only if all partial verdicts are 'pass' as well.

The demonstration of the technical competence to the evaluation authority task may be fulfilled by the evaluation authority analysis of the output tasks results, or may include the demonstration by the evaluators of their understanding of the inputs for the evaluation sub-activities. This task ends with the evaluator authority verdict.

This description of evaluation process is summarized in the action flow and presented using BPMN 2.0 notation (see Figure 8 below).

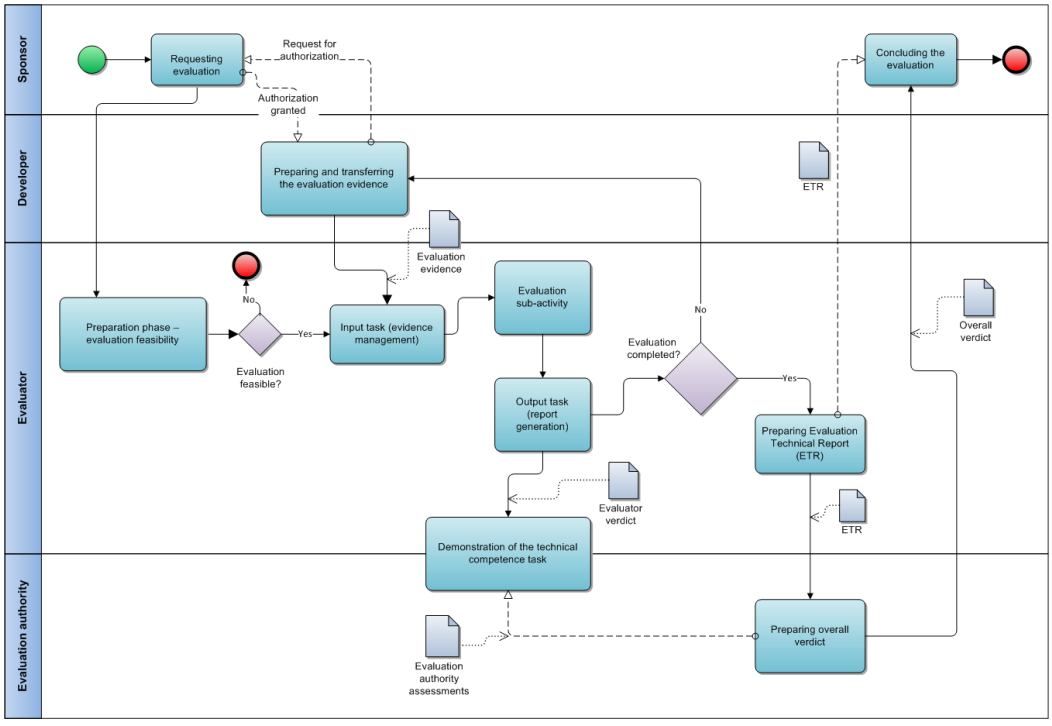


Figure 8: The evaluation process according to ISO/IEC TR 18045

5.3 Requirements for laboratories operating in international schemes

5.3.1 CCRA

An Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security (CCRA)[14] imposes several requirements on the laboratories (called here 'Evaluation Facilities'). In general, laboratories shall be:

- either accredited by relevant accreditation body in accordance with ISO/IEC 17025, or
- established under the laws, statutory instruments, or other official administrative procedures valid in the country concerned.

In both cases, common requirements apply, as specified in one of the Annexes[15] of CCRA. In particular, the laboratory shall be licensed or otherwise approved by the Certification Body. Furthermore, the Evaluation Facility also has to demonstrate that it is technically competent in the specific field of IT security evaluation and that it is compliant with the rules of the scheme concerned.

Finally, the CCRA states each scheme can establish its own requirements in relation to security, personnel training and operating procedures. Differences among schemes with regard to requirements for laboratories are discussed in Chapter 4.

Apart from the arrangement itself, CCDB[16] publishes supportive documents, mandatory for use by the laboratories, which include requirements for the evaluator's activities in specific areas of evaluation such as Stateful Traffic Filter Firewalls or Integrated Circuits. Full list of supportive documents (SDs) is presented in the CCRA official web site[17].

5.3.2 SOGIS-MRA

This arrangement provides the same general requirements for laboratories as the CCRA. However, due to narrower scope of operation than CCRA, and higher requirements with regard to assurance, there are additional obligations imposed on laboratories. These obligations are described in two documents:

- *Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices*[18],
- *Minimum ITSEF Requirements for Security Evaluations of Hardware Devices with Security Boxes*[19].

The first document contains several requirements concerning:

- basic and detailed knowledge and experience of evaluators in several areas related to Integrated circuit (IC) technology, including: the IC design and production processes, security of IC devices and

[14] https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf
[15] namely, Annex B.3 *Accreditation and Licensing of Evaluation Facilities*
[16] CCDB – Common Criteria Development Board manages the technical work program for the maintenance and ongoing development of the CC and CEM and reach agreement on the application of the CC and CEM to evaluations.
[17] https://www.commoncriteriaportal.org/cc/#supporting
[18] https://www.sogis.org/uk/supporting_doc_en.html
[19] This document is not publicly available

the environment they are operating, hardware physical and software-related attack techniques that could compromise a secure IC, cryptography techniques used in the ICs,
- the evaluators' ability to use dedicated hardware and software tools to perform attacks against the IC components, and further to analyse the data gathered as a result of data-capture and signal processing procedures.

Additionally, the document lists types of equipment indispensable for performing specific attacks against the ICs and similar devices, and discuss the way the laboratory can use them. Furthermore, it describes required capabilities of the laboratory to perform composite evaluations of software and hardware of the product, in terms of tools and necessary equipment.

Finally, the document contains basic requirements to the organization of the evaluations and use of subcontractors.

The second document discusses similar topics but in relation to another technical domain ie. hardware devices with security boxes (sometimes called 'hardware security modules' - HSM). It includes specific requirements with regard to:

- the evaluators, in terms of their skills and experience i.e:
  - basic knowledge in the area of electricity and chemistry,
  - detailed knowledge and experience of design principles of integrated circuits, microcontroller architecture, functionality and packaging, several attack techniques against the hardware and programmable micro-controllers, cryptographic algorithms and random number generators,
  - ability to use the equipment to perform independent tests and attacks.
- the laboratory unrestricted access to dedicated facilities such as
  - 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)
- the laboratory organization for evaluations, in term of the use of bespoken equipment, directly or by subcontracting.

Additionally, it should be noted there are several detailed supporting documents for evaluations, mandatory to use for laboratories under the SOGIS MRA. These are listed in Table 199.

	NAME OF THE SOGIS MRA DOCUMENT
1.	Application of Attack Potential to HW Devices with Security Boxes (for trial use)
2.	Application of Attack Potential to POIs
3.	Application of Attack Potential to Smartcards
4.	Application of CC to Integrated Circuits
5.	Attack Methods for HW Devices with Security Boxes
6.	Attack Methods for POIs
7.	Attack Methods for Smartcards and Similar Devices
8.	Collection of Developer Evidence
9.	Composite product evaluation for Smart Cards and similar devices
10.	ETR for composite evaluation template
11.	Guidance for Smartcard evaluation
12.	CEM Refinements for POI Evaluation
13.	Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices – Appendix 1
14.	Security Evaluation and Certification of Digital Tachographs
15.	Certification of "open" smart card products

Table 199: Review of the SOGIS MRA documents which supports security evaluations

5.4 Standards supporting specific areas of evaluation

5.4.1 Standards in support of evaluation methods and techniques

There are several types of IT products which require various methods, techniques, tools and procedures for security evaluations. Consequently, specific and detailed knowledge, skills and experiences are expected from evaluators in these areas as well.

Several standards which support the evaluation methodology as described in ISO/IEC TR 18045, in particular for vulnerability assessments, are listed in Table 200.

STANDARD NUMBER	STANDARD TITLE
ISO/IEC 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
ISO/IEC TR 20004:2015	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
ISO/IEC TS 30104:2015	Physical security attacks, mitigation techniques and security requirements
ISO/IEC 19790:2012	Security requirements for cryptographic modules
ISO/IEC 19792:2009	Security evaluation of biometrics
ISO/IEC 17825:2016	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
ISO/IEC 18367:2016	Cryptographic algorithms and security conformance testing
ISO/IEC 20540*	Guidelines for testing cryptographic modules in their operational environment
ISO/IEC 24759:2015	Test requirements for cryptographic modules
ISO/IEC 29128:2011	Verification of cryptographic protocols
ISO/IEC 29147:2014	Vulnerability Disclosure
ISO/IEC 30111:2011	Vulnerability handling processes
ISO/IEC 30107-3:2017	Biometric presentation attack detection -- Part 3: Testing and reporting
*awaiting publication	

Table 20: Review of International standards related to security evaluations of various types of ICT products

It should be noted there is undergoing constant development of standards in new areas of applicability of security evaluations such as white-box cryptography, quantum cryptography, patch management and deployment activities[20].

5.4.2 European standards supporting security evaluations

Significant standardization activities are related to the implementation of Regulation No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market[21] (eIDAS).

According to the Commission Implementing Decision No 650/2016 laying down standards for the security assessment of qualified signature and seal creation devices (...)[22], ISO/IEC 15408, part 1-3, and ISO/IEC 18045 are designated as the reference documents for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices or qualified electronic seal creation devices. Further, the decision refers to multi-part European Standard EN 419211 *Protection profiles for secure signature creation device,* containing subjects for evaluations and subsequent certifications ie. Protection Profiles for relevant electronic signature/electronic seal devices (see Table 221).

[20] Based on the ISO/IEC JTC1/SC27 Programme of Work, document not publicly available
[21] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[22] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650

EN 419211 PART	EUROPEAN STANDARD TITLE
EN 419211-1:2014	Overview
EN 419211-2:2013	Device with key generation
EN 419211-3:2013	Device with key import
EN 419211-4:2013	Extension for device with key generation and trusted channel to certificate generation application
EN 419211-5:2013	Extension for device with key generation and trusted channel to signature creation application
EN 419211-6:2014	Extension for device with key import and trusted channel to signature creation application

Table 221: European Standards referenced in the Commission Implementation Decision no 650/2016

There are other European Standards, not referenced in the Decision 650/2016, which are relevant for performing security evaluations of electronic signature related devices such as these included in Table 22.

EN NO	STANDARD TITLE
EN 419212	Application Interface for smart cards used as Secure Signature Creation Devices
EN 419212-1:2014	Basic services
EN 419212-2:2014	Additional services
EN 419251	Security requirements for device for authentication
EN 419251-1:2013	Protection profile for core functionality
EN 419251-2:2013	Protection profile for extension for trusted channel to certificate generation application
EN 419251-3:2013	Additional functionality for security targets

Table 22: European Standards related to the ISO/IEC 15408 and ISO/IEC 18045

6. Practices of laboratories

6.1 Typical processes and timeframes for evaluation

The evaluation according to Common Criteria usually happens in a typical ping-pong run. The developer provides evidence to the evaluation laboratory that the product (the Target of Evaluation, to be more precise) meets certain requirements as determined in the Security Target documentation; the laboratory reviews and tests the evidence and provides feedback to the developer. Relevant documentation and the TOE itself are revised and the process starts over.

Evaluations are typically organized by examining several assurance classes separately. This means that the following areas of an evaluation are addressed one after the other:

- The Security Target specification
- The Design Documentation (Class ADV)
- The Guidance Documentation (Class AGD)
- The Life-Cycle Documentation (Class ALC)
- Testing and Vulnerability Analysis (Class ATE and AVA)

In the context of the international recognition of the criteria and the overall complexity of the Target of Evaluation, some of the documentation to be provided for an evaluation can get complex. In this context, it is common that the evaluation/testing of a certain piece of information or its revision takes several weeks rather than few days.

The overall timeframe that needs to be planned for an evaluation depends on the following factors (in that order):

- The chosen Evaluation Assurance Level (EAL). The basis for the estimations is the list of work units from [ISO18045] that relate to the chosen EAL.
- The complexity of the Target of Evaluation
- The experience of the developer
- The experience of the lab and
- the maturity of the criteria

The question of the overall timeframe of an evaluation is hard to answer but the following lists should provide a first overview:

Timeframes after EAL:

- EAL 1,2,3: evaluations typically can take less than 6 months
- EAL 4: evaluations are typically planned in a timeframe of a year
- EAL 5 and above: 1 1/2 years and above

In this context, it should be noted that the listed timeframes should just be taken as examples based on the experience of the editors. Timeframes vary significantly from scheme to scheme and are even restricted by some schemes (e.g. in the US).

Timeframe considering the complexity of the product:

- Simple products: See above

- Products of medium complexity: add 10-20%
- Complex products: add 50 % or more

The experience of the developer plays a very important part regarding the schedule of an evaluation. A well experienced developer can easily cut the timeframes that have been mentioned before even by half, specifically if a predecessor version of the product already has been certified. On the other hand, novices in the field of Common Criteria, are well advised to allow some extra time in their schedule.

The experience of the evaluation laboratory and the maturity of the evaluation criteria are two influencing factors that are less often discussed. Even though, no reliable data exists for this question, empirical observations lead to the conclusion that the experience of the laboratory has significant impact on the timeframe of an evaluation. This does not only refer to the experience of the laboratory in general (meaning how many evaluations a laboratory has carried out) but it specifically refers to the experience of the laboratory with respect to similar products. As an example: A laboratory that has already performed evaluations of firewalls according to a certain Protection Profile will have a significant advantage for evaluations in this area (even over other labs that are more experienced in general but have less specific experience).

Last, but not least, the maturity of the criteria is an important aspect. This does not relate to the maturity of the Common Criteria itself but relates more to the maturity of dedicated Protection Profiles, interpretations and guidance documents. Specifically, when these criteria are used for the first time, evaluations usually take significantly longer.

6.2 Operational procedures

Operational procedures for working in a laboratory should be seen in different contexts as follows:

- Working as an evaluator
- Working as a lead/senior evaluator
- Managing a laboratory

The work of an **evaluator** comprises the review of the documentation that has been provided by the developer as well as tests and vulnerability assessment of the product itself. In larger laboratories, it is common that evaluators specialize in certain aspects of evaluation procedures. Even though it is usually the case that evaluators are capable to conduct all aspects of an evaluation, they often focus on certain aspects of an evaluation in their daily work.

From the evaluator perspective, the daily work is characterized by the four-eyes principle that is inherent to the Common Criteria requirements in many different places. Every step of work that is performed by the evaluator is typically reviewed by at least one competent co-worker. The extensive amount of reviews and checks facilitates the high quality of the evaluation procedures according to Common Criteria.

Every evaluation is led by a **senior/lead evaluator**. The work in such role usually includes strict and active supervision of the evaluator but is augmented by aspects of project management and customer relations. The senior evaluator should be a well experienced professional and therewith is the first point of contact for all evaluators in a project if questions arise. Also, it is typical that sensitive decisions and test results that potentially have an impact on entire evaluation are discussed and double-checked with the senior/lead evaluator.

The senior/lead evaluator overlooks the entire project and also consider the effect of a technical decision on the overall project schedule and budget. Also, senior/lead evaluators usually are responsible for

contacting customers, establishing modes of co-operation, leading milestone meeting and similar activities.

The manager of the laboratory oversees all evaluation processes which are conducted in that laboratory. With respect to the evaluation processes themselves, the lab manager represents another level of escalation. If a technical dispute among evaluators (or between evaluators and the developer or sponsor) comes up, the lab manager can be involved. However, in a large number of laboratories, the position of a lab manager is seen as a management position rather than a technical one. This means that a lab manager does not necessarily have the technical background and knowledge to discuss all technical issues. The primary focus of the lab manager in daily life is:

- to ensure that the laboratory follows all regulations,
- to ensure that new interpretations and information about the Common Criteria are circulated amongst all evaluators and utilized during evaluations,
- to communicate with the certification and accreditation authorities in all substantial issues with regard to the accreditation of licensing of laboratory.

6.3 Capacity and capabilities

Gaining an overview of the capabilities of all evaluation laboratories in Europe that work in the area of Common Criteria is not an easy task. The main reasons for this are:

1) There is no obligation for a certification or evaluation authority to report on finished certification.
2) Evaluations can remain unreported for a variety of reasons as such:
   a. The evaluation fails,
   b. The evaluation is performed in the context of confidential project (e.g. a project with military scope or a classified project, in general)
3) The primary, central source for certifications under www.commoncriteriaportal.org often remains obsolete.

The analysis in this chapter is based on the information as published on www.commoncriteriaportal.org and augmented by the knowledge of the experts who authored this report.

By the time this report has been prepared (November 2017) a total of 1864 certificates have been reported under www.commoncriteriaportal.org by European laboratories.

Over the last few years, the numbers are as follows:

- 2016: 83 certificates
- 2015: 147 certificates
- 2014: 163 certificates

When looking at these numbers, one should keep in mind that quite a few of these products the certificates are granted to, have actually been re-certified.

The following table shows, how the certificates in 2014-2016 are distributed over the European countries that issue certificates:

	2014	2015	2016	TOTAL
Germany	62	46	11	878
Spain	7	7	8	80
France	75	57	57	777
Italy	1	8	3	21
thNetherlands	5	12		45
Sweden	6	7	3	21
UK	7	10	1	41

Table 23: Number of certificates per country 2014-2016

The following figures show how the published certificates are distributed among the various classes of products (the most populated categories shown for clarity of presentation).

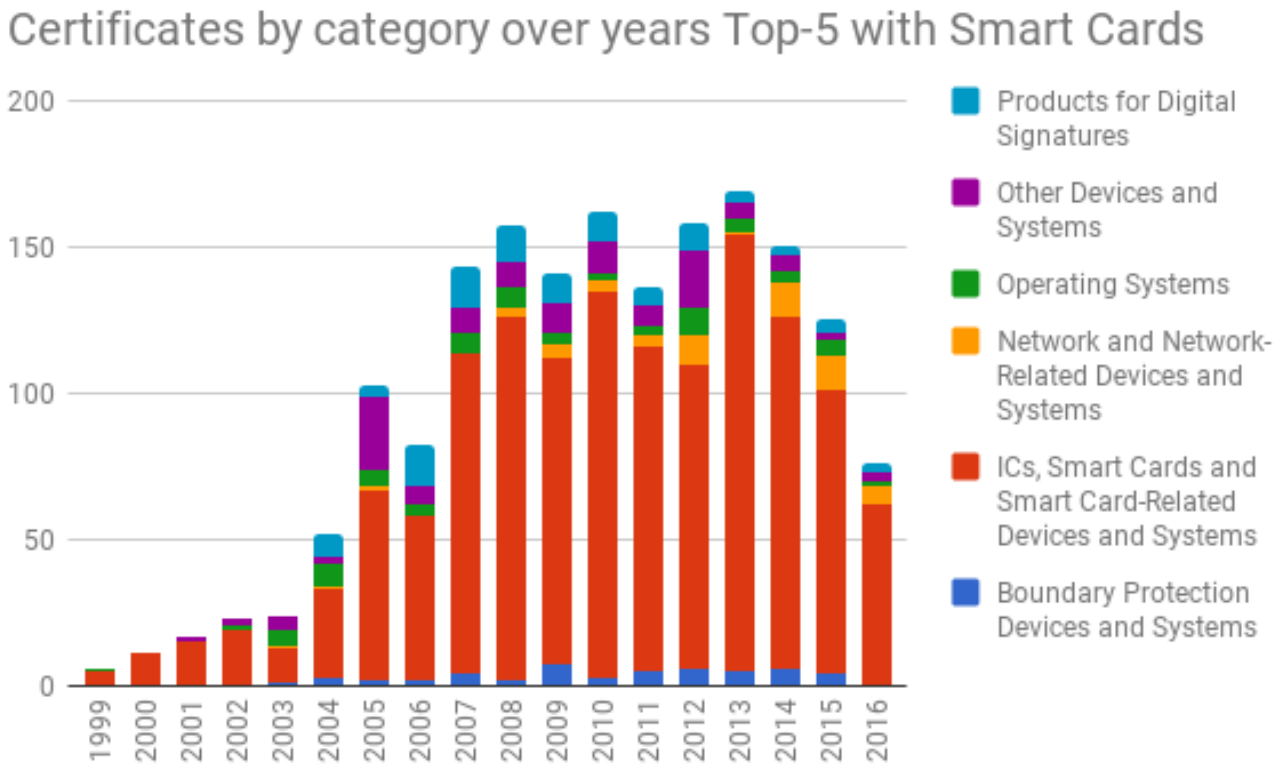


Figure 9: Number of certificates by category

It becomes immediately obvious that the vast majority of certificates are issued for smart cards and similar devices.

If one filters out the smart card related certificates (see Figure 10) and repeats the analysis, the next top 3 are not so obvious as they change over the years. However, it's probably fair to say that the next most popular categories for certification are databases, products for digital signatures and network devices.

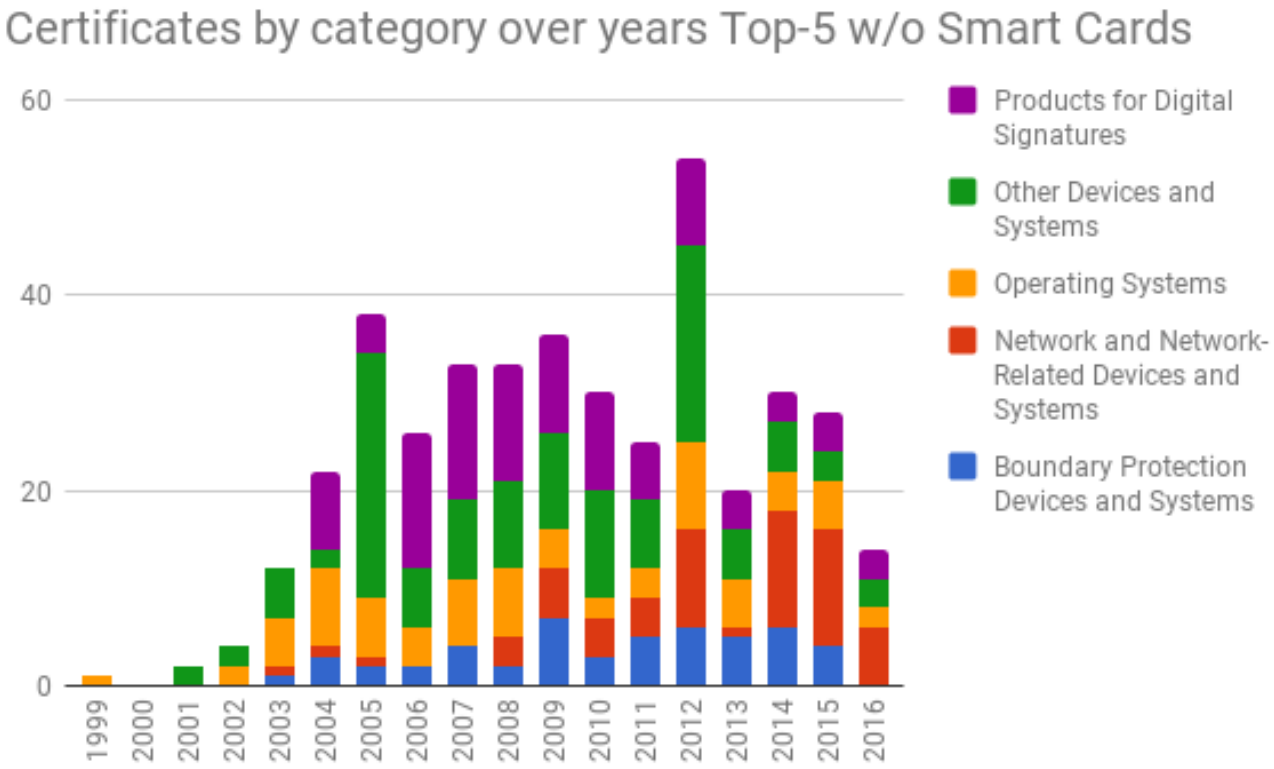


Figure 10: Numbers of certificates by category w/o smart cards

6.4 Personnel

A plethora of requirements that have to be met by the personal are covered by the criteria as introduced previously. In this context, it falls into the responsibility of the certification body to ensure that evaluation labs meet the requirements. This includes competence requirements for evaluators. In this context, some certification authorities also have documented criteria that summarize the requirements.

While developing this report, investigation has also been performed with respect to the question, how the various schemes address the requirements on personnel. The outcome of this investigation can be found in Table 22

COUNTRY	CERTIFICATION BODY (CB)	PRIVATE COMPANY	EVALUATION FACILITY (EF) NAME	REQUIREMENTS FOR EVALUATORS
UK	National Cyber Security Centre (NCSC)	Commercial Evaluation Facility (CLEF)	Commercial Evaluation Facility (CLEF)	3 levels of qualification: Trainee evaluator (successful training, which is APPROVED by the CB and CONDUCTED by a Qualified Evaluator [or Specialist if appropriate field]); Qualified evaluator (a Trainee Evaluator who has been assessed by the CB to be capable of evaluation work w/o supervision; Specialist evaluator (assessed as Qualified for some subset of the CC Assurance Classess, for others he/she is equivalent to a Trainee). Assessment for Qualified and Specialist based

				on a positive recommendation by the CLEF managment and written reports produced by the Trainee Evaluator [inc trail evaluation]
Australia & New Zealand	Australasian Certification Authority	Australasia IT Evaluation Facility (AISEF)	Australasia IT Evaluation Facility (AISEF)	every evaluator has to be approved by ACA (CV for approval); AISEF CC training
Sweden	Swedish Certification Body for IT Security (CSEC)	IT Security Evaluation Facilities (ITSEF)	IT Security Evaluation Facilities (ITSEF)	two levels: Evaluator (works under Qualified Evaluator's supervision) and Qualified Evaluator (Evaluator assessed by the CB and meets the requirements); the head of ITSEF applies for a staff member to be Evaluator or Qualified Evaluator (with CV and declaration of competence); candidate for Evalutor status shall complete the CC training offered by the CB and pass the CC/ Scheme examination, for a Qualified Evaluator: Evaluator's progress is monitored by the CB, the Evaluator shall demonstrate experience in planning and conduct evaluation activities and at least once have independently written Evaluator results for all Evaluator actions in each assurance family at EAL4 or higher
Canada	Communications Security Establishment (CSE)	Common Criteria Evaluation Facilities (CCEF)	Common Criteria Evaluation Facilities (CCEF)	staff members of the Company shall possess a Certificate of Evaluator Approval, issued by the CB (conditioned on positive assessment of the CV and passing of the CC Evaluator Exam)
Germany	Bundesamt fuer Sicherheit in der Informationstechnik (BSI)	CC-Pruefstellen	CC-Pruefstellen	each of individual evaluators is recognized by CB, after assessment of their competence and completion of a BSI-conducted training, all evaluators must participate in a trial evaluation (on a fictional case)
The Netherlands	TUV Rheinland Nederland and the Ministry of the Interior and Kingdom Relations	ITSEF	ITSEF	CC training course (either by the CB or approved by the CB) concluded with an examination. Passing the exam results in a licesed Evaluator status
USA	National Information Assurance Partnership (NIAP)	Common Criteria Testing Laboratories (CCTL)	Common Criteria Testing Laboratories (CCTL)	No NIAP requirements in terms of personnel; NIST (NCLAP) accreditation lists requirements for the personnel, including education, skills, training - all responsibility of the laboratory, assessed by NIST during accreditation reviews
Malaysia	Malaysian Common Criteria Certificaton Body (MyCB)	Malaysian Security Evaluation Policy (MySEF)	Malaysian Security Evaluation Policy (MySEF)	Senior MySEF evaluator: at least 2 years of CC evaluation or certification expierenece, MS ISO/IEC 17025 and its application to MySEF operations, recognised as an Authorised signatory for Department of Standards Malaysia or any Accredited Body; MySEF evaluator must show pre-requisite knowledge (by tertiary qualifications, professional certifications or equivalent expierence)
Japan	IT Promotion Agency Japan (IPA)	Commercial Evaluation Facility (CEF)	Commercial Evaluation Facility (CEF)	qualified evaluator (at least one) (qualification by means of a trial evaluation), training

				provided by the CEF with a certificate of completion
Norway	SERTIT	ITSEF	ITSEF	one of the tasks of the SERTIT is "keeping an overview of the professional status of the employees of an ITSEF"
France	Anssi	ITSEF	ITSEF	ANSSI is responsible for the assessment of the capability of the evaluation facility relating to the scope of its license. At the request of the CB ITSEF must present evidence that its staff skills meet the scope

Table 22: Requirements on Personnel

The results in this table show that the actual requirements on personnel for CC certifications differs among the various schemes. In order to facilitate a harmonization of the requirements in this context, ISO/IEC SC27 WG3 has started a project in this area. The three-part standard ISO/IEC 19896-1,2,3 Information technology — Security techniques — Competence requirements for information security testers and evaluators comprises the following parts

- Part 1 introduces the general concept and some general requirements
- Part 2 specifies Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
- Part 3 specifies Knowledge, skills and effectiveness requirements for ISO/IEC 15408 (Common Criteria) evaluators

The international standardization of these requirements in the context of ISO will lead to a further harmonization of the competence requirements for evaluators in different fields that will - in the end -also help to improve the quality and comparability of evaluations in general.

Annex A: List of full members of EA[23]

Albania	**DPA** Directorate of Accreditation Drejtoria e Pergjithshme e Akreditimit Str Sami Frashri, No.33 1001 Tirana Phone: +355 4 22 69 325 Fax: - Website: www.dpa.gov.al E-mail: armond.halebi@dpa.gov.al *Re-evalutation within 2 years after initial evaluation*
Austria	**AA** Akkreditierung Austria Federal Ministry of Science, Research and Economy Division I/12 Stubenring 1 A 1010 VIENNA Phone: +43 1 71 100 805411 Fax: +43 1 71 100 8045411 Website: www.bmwfw.gv.at/akkreditierung E-mail: akkreditierung@bmwfw.gv.at
Belgium	**BELAC** Belgian Accreditation Council Federal Public Service Economy - Division Accreditation 16, Boulevard du Roi Albert II 2nd floor B-1000 Brussels Phone: +32.2 27 75 434 Fax: +32.2.27 75 441 Website: www.belac.fgov.be E-mail: belac@economie.fgov.be
Bulgaria	**BAS** Executive Agency "Bulgarian Accreditation Service" 52A Dr. G.M. Dimitrov blvd. 1797 Sofia Phone: +359 2 873 53 02 Fax: +359 2 873 53 03 Website: www.nab-bas.bg E-mail: office@nab-bas.bg
Croatia	**HAA** Croatian Accreditation Agency Ulica grada Vukovara 78 10000 ZAGREB Phone: + 385 1 610 6322 Fax: +385 1 610 9322

[23] European co-operation for Accreditation, http://www.european-accreditation.org

	Website: www.akreditacija.hr E-mail: akreditacija@akreditacija.hr
Cyprus	**CYS-CYSAB** Cyprus Organization for the Promotion of Quality Ministry of Energy, Commerce, Industry and Tourism 13-15 A. Araouzos Str. 1421 NICOSIA Phone: +357 22 409 353 or 357 22 409 310 Fax: +357 22 754 103 Website: www.cys.mcit.gov.cy E-mail: aioannou@cys.mcit.gov.cy
Czech Republic	**CAI** Czech Accreditation Institute Olsanska 54/3 CZ-130 00 PRAGUE 3 Phone: +420 272 096 222 Fax: +420 272 096 221 Website: www.cai.cz E-mail: mail@cai.cz *Signed PTP for the 1st time in 04/2017*
Denmark	**DANAK** Danish Accreditation Dyregaardsvej 5B 2740 Skovlunde Phone: +45 77 33 95 00 Fax: +45 77 33 95 01 Website: www.danak.org E-mail: danak@danak.dk *Signed PTP for the 1st time in 04/2017*
EAK	**EAK** Estonian Accreditation Centre Mäealuse 2/1 12618 Tallinn Phone: + 372 6 021 801 Website: www.eak.ee E-mail: info@eak.ee
Finland	**FINAS** Finnish Accreditation Service P.O. Box 66 Opastinsilta 12 B 00521 HELSINKI Phone: + 358 29 5052 000 Website: www.finas.fi E-mail: akkreditointi@finas.fi *Signed PTP for the 1st time in 04/2017*
France	**COFRAC** Comité français d'accréditation 52 rue Jacques Hillairet 75012 PARIS Phone: (33) 01.44.68.82.20 Fax: (33) 01.44.68.82.21 Website: www.cofrac.fr

	E-mail: information@cofrac.fr *Signed PTP for the 1st time in 04/2017*
Germany	**DAkkS** Deutsche Akkreditierungsstelle GmbH Spittelmarkt 10 10117 Berlin Phone: +49 (0) 30 67 059 10 Fax: +49 (0) 30 67 0591 90 Website: www.dakks.de E-mail: contact@dakks.de
Greece	**ESYD** Hellenic Accreditation System 7 Thisseos str 17676 Kallithea ATHENS Phone: + 30 210 7204 502 Fax: + 30 210 7204 501 Website: www.esyd.gr E-mail: esyd@esyd.gr *Signed PTP for the 1st time in 04/2017*
Hungary	**NAH** National Accreditation Authority Tétényi út 82 1119 Budapest Phone: +36 (1) 203-3981 Fax: +36 (1) 204-5075 Website: www.nah.gov.hu E-mail: titkarsag@nah.gov.hu *04/2017 for inspection*
Iceland	**ISAC** Icelandic Board for Technical Accreditation Einkaleyfastofan Engjateigur 3 IS-150 REYKJAVIK Phone: +354 580 9400 Fax: +354 580 9401 Website: www.isac.is E-mail: isac@isac.is
Ireland	**INAB** Irish National Accreditation Board Metropolitan Building James Joyce Street Dublin 1 Dublin Phone: 00 353 1 6147152 Website: www.inab.ie E-mail: inab@inab.ie *Signed PTP for the 1st time in 04/2017*
Italia	**ACCREDIA** Ente Italiano di Accreditamento Via Guglielmo Saliceto, 7/9 00161 Roma

	Phone: +39 06 8440991 Fax: +39 06 8841199 Website: www.accredia.it E-mail: trifil@accredia.it *Signed PTP for the 1st time in 04/2017*
Latvia	**LATAK** Latvian National Accreditation Bureau 157, kr.Valdemara Str. LV - 1013 RIGA Phone: + 371 67373051 Fax: + 371 67362990 Website: www.latak.lv E-mail: administracija@latak.lv
Lithunia	Lithuanian National Accreditation Bureau T. Kosciuskos st. 30 01100 Vilnius Phone: +370 706 65173 Fax: +370 706 64602 Website: www.nab.lt E-mail: info@nab.lt
Luxemburg	**OLAS** Office Luxembourgeois d'Accreditation et de Surveillance 1, avenue du Swing L-4367 BELVAUX Phone: +352 24 77 43 00 Fax: +352 24 77 93 10 Website: www.ilnas.public.lu E-mail: dominique.ferrand@ilnas.etat.lu
Malta	**NAB-Malta** National Accreditation Board -*Signatory in testing except ISO 15189 Mizzi House National Road HMR9010 Blata l-Bajda Phone: + 356 21 255548 Fax: + 356 21 242406 Website: www.nabmalta.org.mt E-mail: claudio.boffa@nabmalta.org.mt
Montenegro	**ATCG** Accreditation Body of Montenegro Ul. Dzordza Vasingtona 51 20000 Podgorica Phone: 382 81 246 279 Fax: 382 81 246 283 Website: www.atcg.co.me E-mail: atcg@co.me
Norway	**NA** Norsk akkreditering Skedsmogata 5 NO - 2000 LILLESTRØM Phone: + 47 64 84 86 00 Website: www.akkreditert.no

	E-mail: akkreditert@akkreditert.no *Signed PTP for the 1st time in 04/2017*
Poland	**PCA** Polskie Centrum Akredytacji ul. Szczotkarska 42 01-382 Warszawa Phone: +48 22 355 70 00 Fax: +48 22 355 70 18 Website: www.pca.gov.pl E-mail: sekretariat@pca.gov.pl *Signed PTP for the 1st time in 04/2017*
Portugal	**IPAC** Instituto Português de Acreditação, I.P. Rua António Gião, 2 - 4º 2829-513 Caparica Phone: +351 212 948 201 Fax: +351 212 948 202 Website: www.ipac.pt E-mail: acredita@ipac.pt
Romania	**RENAR** Romanian Accreditation Association 242, Calea Vitan sector 3 031301 Bucharest Phone: + 40 21 402 04 71 Fax: + 40 21 402 04 89 Website: www.renar.ro E-mail: renar@renar.ro
Serbia	**ATS** Accreditation Body of Serbia Vlajkoviceva 3 11000 BEOGRAD Phone: + 381 11 313 03 73 Fax: + 381 11 313 03 74 Website: www.ats.rs E-mail: office@ats.rs
Slovakia	**SNAS** Slovak National Accreditation Service P.O. Box 74 Karloveska 63 SK 840 00 BRATISLAVA Phone: + 421 948 349 517 Website: www.snas.sk E-mail: snas@snas.sk
Slovenia	**SA** Slovenska akreditacija - * Signatory in testing except ISO 15189 Šmartinska 152 1000 Ljubljana Phone: +386(0)15473250 Fax: +386(0)15473272

	Website: www.slo-akreditacija.si E-mail: dejana.robic@slo-akreditacija.si
Spain	**ENAC** Entidad Nacional de Acreditación Serrano, 240 28016 MADRID Phone: + 34 91 457 3289 Fax: + 34 91 458 6280 Website: www.enac.es E-mail: enac@enac.es *Signed PTP for the 1st time in 04/2017*
Sweden	Swedish Board for Accreditation and Conformity Assessment Box 878 SE - 501 15 BORAS Phone: + 46 33 17 77 00 Fax: + 46 33 10 13 92 Website: www.swedac.se E-mail: merih.malmqvist@swedac.se
Switzerland	**SAS** Swiss Accreditation Service State Secretariat for Economic Affairs SECO Holzikofenweg 36 3003 BERN Phone: + 41 58 463 35 11 Website: www.sas.admin.ch E-mail: info@sas.ch
The former Yugoslav Republic of Macedonia	The Accreditation Institute of the former Yugoslav Republic of Macedonia Kej Dimitar Vlahov No.4, Building 2, floor 3 1000 Skopje Phone: +389 (0)2 3293 080 Fax: +389 (0)2 3293 089 Website: www.iarm.gov.mk E-mail: vesna.georgievska@iarm.gov.mk
The Netherlands	**RVA** Raad voor Accreditatie Daalseplein 101 PO Box 2768 NL-3500 GT UTRECHT Phone: + 31 30 239 4500 Website: www.rva.nl E-mail: jan.vander.poel@rva.nl *Signed PTP for the 1st time in 04/2017*
Turkey	**TURKAK** Turkish Accreditation Agency Mustafa Kemal Mahallesi 2125 Sokak No:1 06520 Çankaya/Ankara Phone: 00 90 312 410 8200 Fax: 00 90 312 410 8300 Website: www.turkak.org.tr

	E-mail: uim@turkak.org.tr *Signed PTP for the 1st time in 04/2017*
United Kingdom	**UKAS** United Kingdom Accreditation Service 2 Pine Trees Chertsey Lane TW18 3HR STAINES-UPON-THAMES Phone: + 44 17 84 42 9000 Website: www.ukas.com E-mail: info@ukas.com *Signed PTP for the 1st time in 04/2017*

Bibliography

[ISO15408]	ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security
[ISO19790]	ISO/IEC 19790:2012 Information technology -- Security techniques -- Security requirements for cryptographic modules
[ISO9000	ISO 9001:2015 Quality management systems -- Requirements
[ISO17025]	ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories
[ISO17065]	ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services
[ISO27000]	ISO/IEC 27000:2016 Preview Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
[ISO17065]	ISO/IEC 17065:2013 Conformity Assessment – Requirements for bodies certifying products, processes and services
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf 02.07.2014

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Catalogue Number: TP-04-18-008-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-248-6
DOI: 10.2824/35439