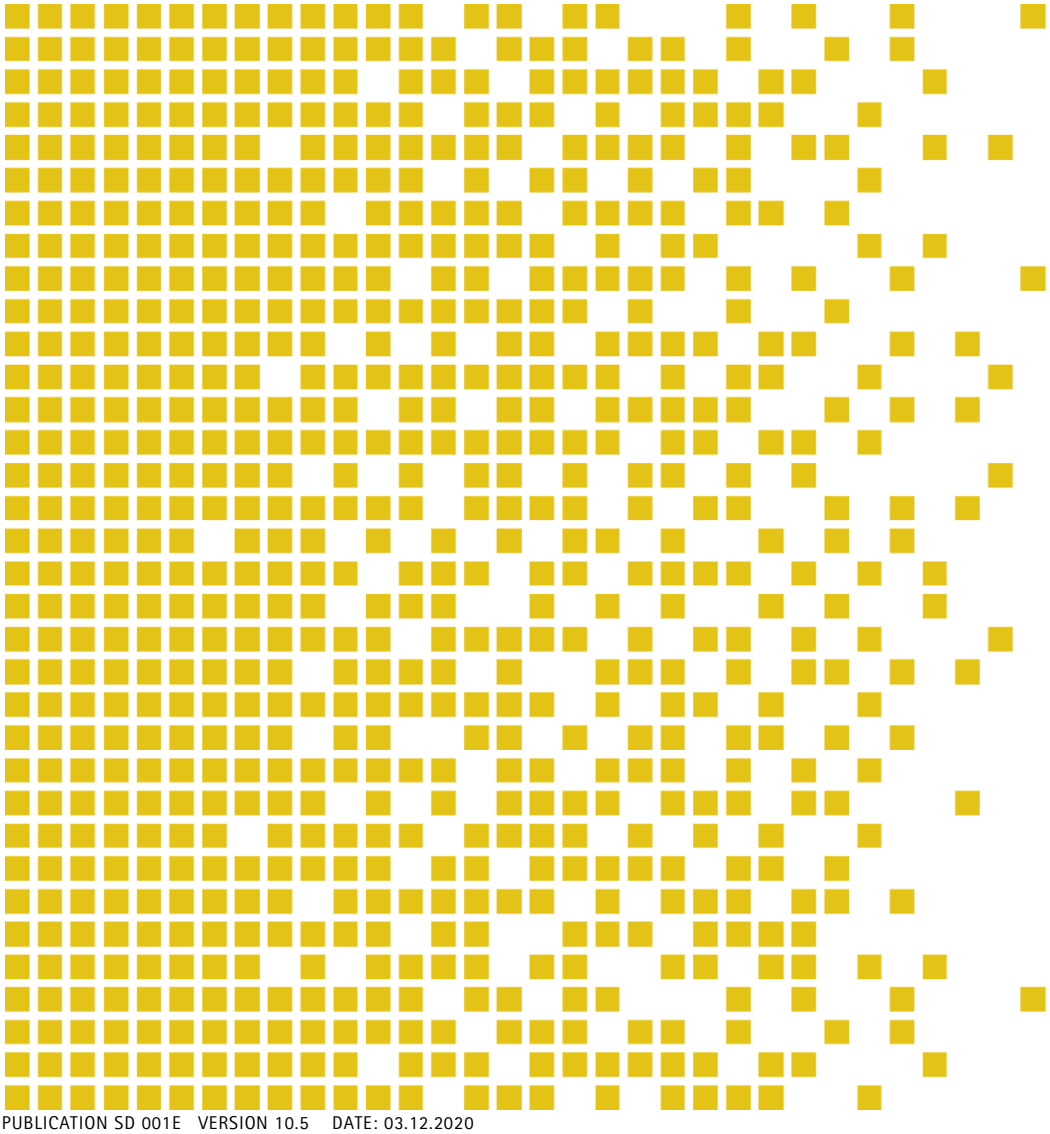
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

The Norwegian Certification Scheme

Evaluation and Certification of IT Security



PUBLICATION SD 001E VERSION 10.5 DATE: 03.12.2020

SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Tel.: +47 67 86 40 00 Internet: www.sertit.no

Document History

Version	*Date*	*Auditor*	*Approved*
10.0	*30.05.2016*	*LB*	~~*HRF*~~
10.3	*30.11.2017*	*LB*	*JAA*
10.4	*20.02.2018*	*LB*	*JAA*
10.5	*03.12.2020*	*LB*	*HN*

Contents

Definition of IT security *v*

1 *Introduction* *1*
1.1 **Frameworks** **3**
1.2 **Mutual Recognition** **3**

2 *Principles for the Certification Scheme* *4*

3 *Organisation and responsibility* *5*
3.1 **SERTIT** **5**
3.2 **IT Security Evaluation Facilities (ITSEFs)** **5**
3.3 **External parties** **6**
3.3.1 Sponsors 6
3.3.2 Developers 6

4 *General provisions* *6*
4.1 **Conducting security evaluations** **7**
4.2 **Framework conditions for evaluation activities** **7**
4.3 **Rules for publishing information** **7**
4.4 **Complaints, disputes and responses** **7**

5 *What can be Certified?* *8*
5.1 **Certification of products (TOE)** **8**
5.2 **Certification of Protection Profiles (PPs or cPPs)** **8**

6 *Preparations for security evaluation and certification* *9*
6.1 **Assumptions for security evaluation** **9**
6.1.1 Notification of engagements and the security evaluation work plan 9
6.1.2 Application for certification 10
6.1.3 Copyright and other rights 10
6.2 **Approval of the certification engagement** **10**
6.3 **Consultative assistance and preparative activities of a security evaluation** **11**
6.4 **Contractual matters** **11**

7 *Security evaluation* *12*
7.1 **Implementation** **12**
7.1.1 Observation reports and activity reports 12
7.1.2 Interaction 13
7.1.3 Oversight 13
7.2 **Evaluation Technical Report** **13**
7.2.1 Protection of information and protection marking of the ETR 14
7.2.2 Company-internal information 14
7.2.3 Assessment and approval of the ETR 14

8 *Certification* *15*
8.1 **The certification process** **15**

8.2 Certification Report 15
8.3 Certificate 15
8.3.1 Rights 16
8.3.2 Certified products 16
8.3.3 Use of Certificates 16
8.3.4 Monitoring Certificates 16
8.3.5 Sanctions in the event Certificates are misused 17

9 Maintenance of the Certificate 17

Abbreviations 18

References 19

Appendix A: History 21

Definition of IT security

To provide an unambiguous understanding of what IT security involves and how it is used in this document, definitions of six key concepts are given below: authenticity, availability, integrity, confidentiality, assurance and accountability. Regulation to information security [1] gives a more complementary definition of information system security and belonging measures.

Authentisity
(Ensure that users are identified and authenticated before access to data and services are given, Prevent introduction of false data and services),

Availability
(Ensure that information and data resources are available to authorised users at the proper time and in the correct form),

Integrity
(Ensure that the information and data resources is correct and is not altered or destroyed by unauthorised persons),

Confidentiality
(Ensure that the information cannot be accessed by unauthorised persons, and that data resources are protected for unwanted usage),

Accountability
(Ensure that incidents relevant for security are detected and registered, and that users can be kept responsible. This also includes non-repudiation).

In other words, IT security is both measures and policy instruments for protecting information that is stored, processed and communicated in IT systems and protection of data resources. Certification is a method to evaluate and set assurance to IT security. It is this understanding of IT security that applies to this document.

1 Introduction

The rapid developments in IT and the growing use and dependency of IT systems in the community, has also during the last years visualised the societies vulnerability of security breakdown in IT systems. It is therefore a need of a better foreknowledge of the various IT products strengths and weaknesses. It may also be a need to compare security traits in a vide variety of products with similar functionality.

Inadequate or misleading information may lead to poor investments or too low IT security.

There are at least three approaches to the evaluation of IT security:

- The first approach is to trust in the supplier's assurances
- The second approach is to conduct one's own tests and evaluations,
- The third approach is to assign the task of assessing the product to an independent third party with the necessary competence.

The first approach may be comfortably, but does not guarantee use of best practice in design and implementation of the security solutions and that the actual weaknesses, faults and shortcomings are detected and corrected. There may be a risk the IT solution lacks the customers satisfactorily level of protection.

The second approach is time-consuming and complicated. Besides, from a societal standpoint, it is hardly expedient for every purchaser to have to spend resources on ascertaining, which maybe is based on different criteria and still not necessarily give satisfactorily assurance of the security level.

The third approach is an independent third party assessment according to international standards. From a societal standpoint, this is a more efficient way of ensuring the assessment once, at one place, and then having the results recognised by many.

For all responsible in the public and private sectors as well as private individuals, it is important to obtain a confirmation of the IT-system security level. It is also important to be able to trust that the IT product has been subjected to an impartial evaluation by a neutral professional body. This is achieved through the establishment of the Certification Scheme.

As the purpose of the Norwegian Certification Scheme is to provide services that support the third approach, the remainder of this document deals exclusively with third party assessment of IT Security.

Norway is member of an international arrangement *"Common Criteria Recognition Arrangement"* (CCRA), cf. section 1.2 ref. [6], and an European Agreement *"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates"* (SOGIS-MRA), cf. section 1.2 ref. [23].

Member states have committed themselves to recognising Certificates issued by qualified certification authorities, so-called “Qualified Participants” (QPs). IT products are to be security evaluated and certified in accordance with the international *Common Criteria (CC)* for evaluation [2], [3] and [4], corresponding to ISO/IEC 15408 [8] and the *Common Evaluation Methodology (CEM)* [5], corresponding to ISO/IEC 18045 [10].

This document describes the public scheme for certification of IT security. in Norway are drawn up The *Norwegian Certification Authority for IT Security* (SERTIT) is given the authority for the Scheme. SERTIT is also responsible for drawing up the framework conditions for the Scheme and execute certification of IT products.

One of the purposes of the Scheme is to meet government and industry sector needs for a cost-effective and efficient security evaluation and certification of IT products.

The point of departure for initiating a certification process may be such as:

- vendor wants to strengthen its market position,
- authorities and business need of assurance to fulfilment of security requirements,
- system developer is required to satisfy conditions in a specific contract,
- purchaser of a product has to comply with the company’s own security requirements, industry standards, or statutory security requirements (issued pursuant to law or regulations).

Other information regarding the certification scheme or any comments shall be addressed to:

The Norwegian Certification Authority for IT Security (SERTIT)
P.O. Box 814
1306 Sandvika

NORWAY

Visiting address: Langkaia 1, Oslo

Phone: +47 67 86 40 00

Internet: sertit.no

1.1 Frameworks

The foundation and authorisation of SERTIT are given in two documents from the Ministry of Trade and Industry of 1 February 1999 and 14 April 1999 both ref. 98/4561-F-IKT eja/lem in the quality system's document list. For further information on the operation and the basis of the IT Security Certification Scheme, please refer to Appendix A.

The Certification Scheme under SERTIT is based on the following international arrangement and agreement of Mutual Recognition of Certificates:

- *"Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security"* (CCRA) [6].
- *"Mutual Recognition Agreement of Information Technology Security Evaluation Certficates"* (SOGIS MRA) [23]

The following national regulatory framework is essential for the involved parties under the Certification Scheme:

- Act relating to protective security services (the Security Act) [21] and belonging regulations,
- Act relating to procedure in cases related to the public administration, (Public Administration Act) [13],
- Act relating to the processing of personal data (the Personal Data Act) [12],
- Instructions for handling of documents in need of protection for reasons other than those mentioned in the Security Act with regulations (the Protection Instructions) [26].

All SERTIT documents mentioned in this document or published on SERTIT's website are part of the framework conditions for the Certification Scheme. Changes in these framework conditions will be published in accordance with the current procedures for the Scheme.

1.2 Mutual Recognition

Norway has committed to conducting security evaluations and certifications in accordance with internationally recognised standards and methods as they are defined in the CCRA [6] and SOGIS MRA [23].

The CCRA and SOGIS MRA contain two key elements:

- All participants are obliged to recognise Certificates according to the applied rules in the CCRA and SOGIS MRA respectively,
- Recognition of qualified certification bodies, *"Qualified Participants (QPs)"* (CCRA) or *"Compliant CBs"* (SOGIS MRA).

In accordance with this, Norway recognises Certificates issued under the CCRA and SOGIS MRA.

Norway has achieved status as Qualified Participant in CCRA and SOGIS MRA, which means the Norwegian Certificates are recognised under these Schemes.

The remainder of this document describes in more detail how the Scheme is set up, the framework pertaining to security evaluation and certification, and how the actual process is carried out.

2 Principles for the Certification Scheme

A central purpose of the Certification Scheme is to ensure evaluations of high and consistent level of quality. The Certification Scheme is grounded in the following principles:

- The Scheme is open and accessible for any applicants,
- Evaluation and Certification shall take place in an impartial and cost-effective way,
- The security evaluation is performed by approved evaluation facilities which operates according to regular business principles,
- SERTIT approves and oversees the evaluation facilities,
- SERTIT decides whether a TOE is appropriate for certification,
- Certificates satisfying the criteria under CCRA or SOGIS MRA are offered mutual recognition,

Evaluation results shall be:

- Provided on basis of unbiased judgement,
- Repeatable and reproducible,
- Complete and technical correctness.

3 Organisation and responsibility

The public scheme for certification of IT security is managed by SERTIT, which is a part of Norwegian National Security Authority (NSM).

The Ministry of Justice and Public Security has the budget responsibility and funds the operation of the NSM. Therefore, SERTIT obtain public finances through NSM.

Section 3.1 - 3.3 describes parties involved in the Certification Scheme, and the parties main tasks and responsibilities.

3.1 SERTIT

SERTIT's main task as the public certification authority for IT security is to issue Certificates and Certification Reports as described in Terms of Reference [20]. SERTIT is also responsible for drawing up rules and framework conditions for the Scheme and for ensuring that the rules are complied with by all parties. SERTIT also oversees the entire evaluation process, which forms the basis for being able to perform certification. SERTIT is also the body that approves commercial evaluation facilities under the public Certification Scheme.

To perform the tasks at SERTIT in an appropriate manner, including meeting the formal requirements [6], [1], [22], [25] and [23], so that the Scheme functions efficiently and effectively, its operations are organised in the following manner:

The Head of SERTIT has the overall responsibility for the day-to-day operation of the Scheme. Certification projects are manned with a project manager, who is also responsible for preparing the Certification Report and Certificate. The quality system shall help the satisfactory performance of certification.

3.2 IT Security Evaluation Facilities (ITSEFs)

IT Security Evaluation Facilities (ITSEFs) that carry out assignments for the Certification Scheme are subject to SERTIT's authority. This means that SERTIT is responsible for approving evaluation activities and subsequently performing verification of the evaluation facility and of all evaluation activities. Evaluation activities are regulated by an operating agreement [19] between SERTIT and ITSEF according to the provisions of the CCRA [6], SOGIS MRA [23] and national framework conditions laid down by SERTIT. ITSEFs must have valid accreditation according to ISO/IEC 17025 [24], and the company must satisfy SERTITs requirements [16] for ITSEFs to get licensed and run business as Evaluation Facility.

The evaluation facilities perform evaluations of PPs (or cPPs) and/or TOE on a commercial basis and documented procedures in accordance with

international standards [2], [3], [4], [5], [8] and [10], arrangement [6] and agreement [23]. ITSEFs perform security evaluations in accordance with documented procedures laid down in a separate quality manual.

Information on approved ITSEFs can be found on website sertit.no.

3.3 External parties

A number of external parties may be involved in the certification process. Most of these are either sponsors or developers, but other actors may be involved as well. Below are a detailed description of these actors and some guidelines for the certification process.

3.3.1 Sponsors

By *sponsor* is meant an organisation or person who requests a certification for a certain IT product. Sponsor's connection to the IT product may vary from a vendor, purchaser, agent acting on assignment from a purchaser, system developer or a consortium representing more than one developer or vendor.

In cases where two or more sponsors are involved, a management group is set up to function as the sponsors' point of contact.

The general framework conditions for the Certification Scheme may place constraints on the contractual relations between the sponsor and the ITSEF.

A sponsor can also be the developer of the IT product or system to be certified. Since in many cases developers use subcontractors, the role of developer is described in greater detail in the section below on Developers.

3.3.2 Developers

By *developer* is meant the company that manufactures the IT product to be certified. In cases where a developer does not have the role of sponsor, co-operation between the parties is required in connection with the evaluation process. The developer is responsible for providing ITSEFs with the necessary technical information on the IT product. The need for information includes access to the documentation necessary for performing the security evaluation and certification.

In some cases, several developers may be involved in a security evaluation, which may result in problems with gaining access to information crucial to the evaluation. Interactions of this type require the parties to enter into the necessary agreements in advance (see also section 6.4).

4 General provisions

This chapter contains some key provisions on Conducting security evaluations, Framework conditions for evaluation activities, Rules for publishing information and Complaints, disputes and responses. Qualified

evaluation facilities or companies intending to become an evaluation facility the public Certification Scheme are pointed to more detailed information in the publication SD 003E [16].

4.1 Conducting security evaluations

The Certification Scheme is based on trust and a neutral professional assessment.

That explains why it is necessary with a formal prior approval from SERTIT in order to start an evaluation engagement under the Scheme.

SERTIT oversees that all security evaluations are conducted by an impartial third party and by qualified personnel.

4.2 Framework conditions for evaluation activities

SERTIT lays down the framework conditions for the application process for authorisation as an ITSEF. These include establishment conditions, selection criteria and financial matters.

The purpose of this is to ensure that the Certification Scheme has adequate capacity in relation to market demand and that it functions efficiently and effectively.

The framework conditions for establishing ITSEFs are described in detail in the document [16].

SERTIT will inform the affected parties about changes in the framework conditions.

4.3 Rules for publishing information

The following provisions relating to the publishing of information on SERTIT, the Certification Scheme or certified products apply to users of the Scheme, such as sponsors, developers and ITSEFs:

- The parties must obtain prior approval from SERTIT when issuing press releases or similar information relating to security evaluations and/or certifications under the Scheme,
- The parties may not make statements in press releases, advertising materials or the like which may contain misleading information on security evaluations and/or certifications, or which may damage the Certification Scheme in any manner.

4.4 Complaints, disputes and responses

NSM by SERTIT is the first level body that handles complaints, disputes and responses related to the Certification Scheme. Any individual decision may be appealed pursuant to the Public Administration Act. Complaints or requests by users of the Scheme for changes in a decision made by SERTIT

must be submitted in writing to NSM by SERTIT. NSM by SERTIT will consider the matter and decide whether the decision is to be upheld or not. If a party appeals a decision made by SERTIT, the matter will be brought before the next administrative level, which will determine if the appeal is to be heard.

All conflicts of a technical nature between sponsors, developers or ITSEFs shall be taken up with SERTIT.

5 What can be Certified?

It is divided between certification of *"Target of Evaluation"* (TOE) and certification of protection profiles expressed either as *"Protection Profile"* (PP) or *"collaborative Protection Profile"* (cPP)[1].

5.1 Certification of products (TOE)

Products to be evaluated are described as *TOE*. The TOE may consist of the entire or a part of the IT product, and the belonging user- and administrative guides. The TOE typically describes a given configuration or several configurations.

The security functions of the product are defined either in a "*Protection Profile" (PP), "collaborative Protection Profile" (cPP)* or a *"Security Target" (ST).* A ST can consist of one or more PPs or based on a cPP. In order to achieve mutual recognition according to CCRA, the ST is required to contain a PP or a cPP. A formal description of the security functions is on of the prerequisites to start a product certification.

Evaluation and Certification of TOE is managed according to the current standard [2], [3], [4], [8], methodology [5], [10] and procedures.

5.2 Certification of Protection Profiles (PPs or cPPs)

Protection Profiles formed as PPs or cPPs describes the generic requirements of a distinct technology area, i.e. a firewall, an operating system or a multifunctional device.

The difference between a PP or a cPP and a ST, is that the latter describes the implementation and realisation of the security functions in a specific product, like a firewall XY, version 1.0.

Evaluation and Certification of PPs and cPPs are managed according to the current standard [2], [3], [4], [8], methodology [5], [10] and procedures.

[1] cPPs are developed by International Technical Communities (iTCs) according to the current framework published on the CCRA website.

6 Preparations for security evaluation and certification

The preparatory phases holds a vide variety of activities before security evaluation and subsequent certification can take place. Most of the activities take place without engagement from the Certification Authority. This includes activities like product development and the belonging documentation. This section describes all activities in interest of the sponsor, ITSEF and the Certification Authority.

6.1 Assumptions for security evaluation

All matters involving security of importance for the security evaluation shall be identified and included in a separate overview. This may include at least the following:

- TOE (hardware, firmware, software),
- PP or cPP,
- ST,
- documentation (technical, user's and administrator's guide),
- technical assistance from the developer,
- access to the developer's premises,
- access to the operating environment,
- tools.

The sponsor is responsible for designing and assuring the quality of ST, deliver necessary documentation, and provide technical assistance from developer and access to the developer premises. The sponsor may use consultancy assistance in ST development.

The ST is to be submitted to the ITSEF and SERTIT for assessment, who determines whether it is sufficient and appropriate to start a security evaluation of the TOE. The sponsor shall be notified in writing of any problems with using the ST submitted before the evaluation starts.

The assumptions have to be satisfied in order to start and carrying out the security evaluation. The ITSEF is responsible for documenting the fulfilment of the assumptions.

6.1.1 Notification of engagements and the security evaluation work plan

ITSEFs are mandated by SERTIT to notify it of new engagements, *"Task Initiation Notice (TIN)",* and to request its approval for conducting security evaluations under the Scheme. This normally occurs after preliminary investigations of the basis for the security evaluation. The procedures for notifying engagements are defined in separate guidelines for ITSEFs.

TIN are to be sent to SERTIT for assessment, after which a start meeting is normally held between the parties. The start up meeting usually takes place after the parties have assessed the existing documentation.

One purpose of the meeting is to ensure that the parties involved are sufficiently familiar with the TOE and have a common understanding of the scope of the certification process.

6.1.2 Application for certification

The sponsor applies to SERTIT for certification on a separate application form [17] which can be downloaded from SERTIT's website.

The application obliges the sponsor to follow all the current rules in the Certification Scheme, and not to subject the Scheme to unlawful or undesirable conditions or otherwise do damage to the Scheme.

To ensure an efficient certification process, it is recommended that the TIN and the application with necessary attachments is sent in one package to SERTIT.

6.1.3 Copyright and other rights

It is normally the developer who retains the copyright to all information on the TOE, and therefore the sponsor does not automatically have access to this type of information. Copyright questions should therefore be regulated in a separate agreement between the parties (see also section 6.4, Contractual matters).

6.2 Approval of the certification engagement

SERTIT may grant an application for certification if there is a fundamental basis to conduct a security evaluation and certification for this being implemented within the framework of the Scheme. This means that the following requirements must be satisfied:

- Certification must be appropriate,
- The formal requirements for certification must be met,
- The security evaluation and certification must be able to be implemented in an impartial manner,
- The security evaluation must be in conformance with the regulations in CCRA and/or SOGIS-MRA, and national regulations,
- According to the TIN, all obligatory evaluation activities must be planned and the plans must reflect a realistic time frame. The plans must contain sufficient resources, including quantities, competence and necessary equipment,
- There must be a high level of probability that all evaluation activities can be carried out as planned.

The commitment may be granted orally at a meeting with the parties, but must subsequently be confirmed by a formal statement. A confirmation shall be given whether the ST, PP/cPP, TOE, and the deliverables as stated in the TIN forms a satisfactorily basis of the proposed security evaluation. Response on the application will be sent to all parties involved.

6.3 Consultative assistance and preparative activities of a security evaluation

The use of consultative assistance for the preparation of a security evaluation is not subject to SERTIT's control and is therefore a case between the sponsor and the client. The use of consultants for development or preparations for an evaluation is normally unproblematic as long as the facility can prove that the requirements for impartiality are being met. Development of ST is an example of preparative activity. The ITSEF should therefore be scrupulous in defining the level of its involvement in solving the problem to ensure that the facility's independent status is not compromised and later does prevent an impartial security evaluation.

SERTIT recommends that the parties sign an agreement that regulates all matters connected with the use of consultants, *inter alia* to ensure that the necessary degree of impartiality is maintained.

In the event of any doubt of impartiality in the case, the ITSEF should contact SERTIT to get the necessary clarification.

6.4 Contractual matters

The sponsor is urged to solicit tenders from several ITSEFs if there is a need for consultative assistance with preparing a security evaluation or planning for a security evaluation and a subsequent certification.

ITSEFs are mandated by SERTIT to enter into an agreement with the sponsor in connection with engagements for security evaluation under the Certification Scheme. Such a binding agreement should exist in advance of evaluation activities. Although it is up to the parties to specify the details of such agreements, it is recommended the following factors are included:

- The need to obtain access to previous evaluation reports.
- Matters related to Assumptions for security evaluation, as specified in section 6.1, like timetables, right of access to information, requirements for storage and the ownership rights to information.
- All matters relating to enterprise-sensitive information.
- All matters connected with the use of consultants, to ensure that the requirements to impartiality are maintained.

It is the sponsor's responsibility to obtain the written permission from the developer to gain access to enterprise-sensitive information as well as to

relinquish its own rights to evaluation results that may compromise such information.

The sponsor may not simply withdraw from a certification assignment once it has begun. SERTIT requires in general that the ITSEF has regulated all matters relating to any breach of contract in a separate agreement for each engagement.

SERTIT decides whether the ITSEF is qualified to carry out a security evaluation under the Certification Scheme. The decision will partly be based on the ITSEF's involvement in the consultancy activities and its capacity to sustain the necessary impartiality.

7 Security evaluation

This chapter describes the main features of the implementation of a security evaluation and the collaboration among the parties in the process. The chapter also describes the steps that go into the preparation of the *Evaluation Technical Report* (ETR).

7.1 Implementation

The technical security evaluation of the TOE and the belonging deliverables is to be carried out in accordance with the approved progress plan. The security evaluation is conducted in accordance with current international regulations through the CCRA, SOGIS MRA, other national framework conditions laid down by SERTIT and the international standards CC and CEM. It is mandatory for the ITSEF to notify SERTIT of all consultancy activities related to the evaluation engagement.

Any changes to the progress plan shall be approved by SERTIT. This to ensure that the proposed work is adequate, that the plans are realistic and that the necessary resources are available. Duties with lack of progress for 6 months may be terminated.

Both ITSEF and the SERTIT must take care that the integrity of the security evaluation is not compromised. By this is meant that the developer shall not have the opportunity to influence the results or prevent an accurate and fair presentation of the results of the security evaluation.

7.1.1 Observation reports and activity reports

The ITSEF shall document on an ongoing basis the results of the security evaluation in activity reports.

If faults and shortcomings are uncovered in the TOE during the security evaluation, this is to be noted in an *Evaluation Observation Report (EOR)*. The EOR shall then be communicated to the sponsor and SERTIT for further consideration.

The sponsor shall respond to the EOR in writing with detailed recommendations for correcting proven faults and shortcomings as well as a timetable for any corrections. The corrections may require adjustments in the deliverables and may have consequences for the progress plan. Viewpoints from SERTIT may be sent on a special review form (RF). The EORs and eventual RFs on the EORs are case documents for the progress meetings (see section 7.1.2.). The process normally proceeds in iterations between the parties until the EORs are resolved. In instances where it is impossible to resolve an EOR problem, please refer to the penultimate paragraph in section 7.1.2, Interaction.

7.1.2 Interaction

Progress meetings for the security evaluation are held between the ITSEF and sponsor. SERTIT convenes and chairs these progress meetings. Besides SERTIT, the ITSEF, developer and sponsor shall attend. The progress plan shall indicate the schedule for the progress meetings.

The ITSEF normally needs to communicate directly with the developer concerning the TOE, deliverables or other matters. Thus, the ITSEF is required to have concluded the necessary agreements with the sponsor concerning such communication.

Discussion of the EOR is a key part of progress meetings. Proposals for resolving problems from the sponsor are discussed by the parties with a view to finding acceptable solutions at the earliest possible stage in the evaluation process. If necessary, an EOR problem can be resolved at the meeting, in which case the conclusion shall be included in the minutes.

If it is not possible to correct the faults or shortcomings, and this will have consequences for the outcome of the certification process, SERTIT shall notify the sponsor of the consequences.

7.1.3 Oversight

As part of its oversight activities, SERTIT may perform the necessary examinations to ensure that the framework conditions for the security evaluation are followed. SERTIT shall also be invited to be present during site-visit and testing.

7.2 Evaluation Technical Report

All security evaluation findings are to be documented in the Evaluation Technical Report (ETR). This report shall be prepared according to current guidelines on a template provided by SERTIT. The framework is based on the requirements given by CCRA, Annex I, SOGIS-MRA and CC/CEM. The ETR constitutes the end product of the ITSEF's work, and forms the basis for the *Certification Report (CR)*.

The conclusions of the ETR are to establish which parts of the evaluation criteria have or have not been met, while providing sufficient evidence for this.

7.2.1 Protection of information and protection marking of the ETR

It must be clearly stated in the report that the contents are to be regarded as business secret information and must not be made public. If the contents do not fall under the Security Act or other national provisions, the ETR must be clearly marked as being business secret information.

As regards the protection of sensitive information in connection with security evaluations and evaluation reports for systems in undertakings subject to the Security Act or corresponding provisions, all information shall be marked as protected in accordance with the provisions in force at the time in question.

The developer may request or require limiting the sponsor's access to company-sensitive information. The ITSEF is responsible to have clearly defined which kind of information shall be protected, and the security rules being obeyed. Both ITSEF and the SERTIT are to ensure that the sponsor does not obtain access to company-sensitive information.

7.2.2 Company-internal information

If the developer has requested that company-internal information is not to be disclosed to the sponsor, the ITSEF is to make sure that the ETR does not contain this kind of information before releasing the report. The ITSEF normally addresses this concern by preparing a short version of the ETR, which is then released to the sponsor for review before it is made public. It should appear on the document whether it is preliminary or final, or whether it has been approved by the certification body.

SERTIT may refuse to carry out certification, if the developer without due cause withholds necessary company-internal information.

7.2.3 Assessment and approval of the ETR

SERTIT reviews the ETR with supporting documents and examines whether the security evaluation has been conducted in accordance with the agreed criteria, methods and procedures in the Scheme, and whether the ETR provides sufficient basis for preparing the Certification Report (CR). SERTIT may examine the belonging work report when necessary.

For the ETR to be approved, all comments must be addressed and the evidence must be sufficient and consistent pursuant to CCRA, SOGIS MRA and CC/CEM requirements.

SERTIT then issues a confirmation that the security evaluation is completed and at the same time informs the parties concerned when the CR is ready to be made public.

8 Certification

This chapter provides a top-level description of the certification process and explains the purpose of the Certification Report (CR) and the Certificate.

The certification process concludes with a formal confirmation of the evaluation results and of whether the evaluation criteria, methods and procedures have been correctly applied. The process for maintenance of the Certificate is described in more detail in Chapter 9.

8.1 The certification process

The certification process begins when there is an approved ETR. As needed, SERTIT may ask the ITSEF for access to particular technical evidence and other results that support the conclusions stated in the ETR. At the same time, ETR and other documents from the security evaluation, observations from testing and results from other supervisory activities constitute important material on which the certification may be based. Sections 8.2 and 8.3 provide a more detailed description of the Certification Report and the Certificate, respectively.

8.2 Certification Report

SERTIT shall document all findings from the evaluation in a Certification Report. The Certification Report may state the Evaluation Assurance Level (EAL) that has been attained, or which Assurance Components are included. The purpose of the Certification Report is to confirm whether the TOE is in compliance with the PP, cPP and/or ST and to identify any vulnerabilities that could be exploited. The Certification Report can recommend suitable countermeasures to neutralise any remaining vulnerabilities. The Certification Report confirms that the security evaluation has been conducted in accordance with the current framework conditions of the Scheme and that the conclusions are consistent and in line with the evidence submitted.

However, the Certification Report provides no guarantee that all faults and shortcomings in the TOE have been revealed.

8.3 Certificate

The Certificate (C) is normally issued with the Certification Report (CR), and serves as a statement of the conclusions made in the CR. The Head of SERTIT gives the final approval of the Certificate and Certification Report.

The issuance of a Certificate does not imply any form of recommendation by SERTIT of the TOE concerned.

The Certificate is valid only for the version, platform and the environment under which the TOE was evaluated.

The sponsor may market a product as certified only when holding a valid Certificate. SERTIT may require that the sponsor provide reference material or documentation that clearly indicates the correct version of the TOE.

8.3.1 Rights

SERTIT holds the copyright on the Certification Report and the Certificate. Reproduction and distribution is permitted provided that the Certification Report is copied in its entirety.

8.3.2 Certified products

SERTIT will regularly publish an overview of products certified under the Scheme. The information will be published on the website to SERTIT and CCRA.

8.3.3 Use of Certificates

The following provisions apply to the use of the Certificate:

- The Certificate may be used only in connection with the product to which the Certificate applies,
- The Certificate may be used only to document the product's compliance with the standards on which SERTIT bases its activities,
- The certification must not be used in an erroneous or misleading manner that brings or may bring SERTIT or the Certification Scheme into disrepute,
- The certification may not be used in advertising or marketing if the Certificate is unvalid or withdrawn,
- The vendor is obliged to have implemented registration and handling of complaints regarding certified products and made these registrations available to SERTIT.

The vendor is obliged to notify SERTIT of any changes to factors that were the object of the security evaluation of the certified product.

For more detailed provisions regarding use of Certificates, users are advised to read the document: Conditions for use of Certificate and Certification Mark [18].

8.3.4 Monitoring Certificates

Monitoring Certificates primarily takes place through a review of information from the sponsor. Statements about certified products in advertising, the media or on the sponsor's website or other matters coming to SERTIT's attention may be made the subject of further investigation.

The purpose of this monitoring is to see to it that the Certificates are used in accordance with the provisions stated in section 8.3.3, Use of Certificates. Certificates are monitored in accordance with defined procedures.

8.3.5 Sanctions in the event Certificates are misused

If Certificates are misused, SERTIT may initiate sanctions pursuant to ISO/IEC Guide 27 [7]. Sanctions are implemented in accordance with defined procedures. The two most common corrective actions are:

- Request for withdrawal of the Certificate,
- Removing the certification mark from the product.

9 Maintenance of the Certificate

A Certificate is valid only for a specific version of a TOE. However, most TOEs undergo changes at a later point of time. These changes are not a part of the scope of the certification. With future changes to a TOE, there is a need for an end-user to have the same degree of confidence in the new version of the TOE as in the original certified version. Therefore the CCRA and SOGIS MRA established framework conditions for maintenance of Certificates, ref. [1] and [22]. Questions related to Certificate Maintenance in SERTIT are addressed in compliance with this framework.

The TOE can, in some circumstances, be part of the Certificate Maintenance programme. The framework conditions are called *"Assurance Continuity"*, and can be downloaded from the CCRA website (www.commoncriteriaportal.org) and SOGIS (sogis.eu) respectively.

For more information of the Maintenance programme, please contact SERTIT.

Abbreviations

CC	Common Criteria
CCRA	Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security
CEM	Common Evaluation Methodology for Information Technology Security
cPP	Collaborative Protection Profile
CR	Certification Report
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
ITSEF	IT Security Evaluation Facility (approved under the Norwegian Certification Scheme)
NSM	Norwegian National Security Authority
PI	Instructions for handling of documents in need of protection for reasons other than those mentioned in the Security Act with regulations (the Protection Instructions)
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement
ST	Security Target
TIN	Task Initiation Notice
TOE	Target of Evaluation

References

[1] CCRA (2012), *Assurance Continuity: CCRA Requirements*, version 2.1, June 2012.

[2] CCRA, *Common Criteria for Information Technology Security Evaluation*, Part 1: Introduction and general model, Current version.

[3] CCRA, *Common Criteria for Information Technology Security Evaluation*, Part 2: Security functional components, Current version.

[4] CCRA, *Common Criteria for Information Technology Security Evaluation*, Part 3: Security assurance components, Current version.

[5] CCRA, *Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Current version.

[6] CCRA (2014), *"Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security"*, 2 July 2014.

[7] ISO (1982), "*Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity"*, ISO/IEC Guide 27:1983, International Organization for Standardization.

[8] ISO, "*Information technology – Security techniques – Evaluation criteria for IT security"*, ISO/IEC 15408, current version, International Organization for Standardization.

[9] ISO (2009), "*Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets"*, ISO/IEC TR 15446:2009, current version, International Organization for Standardization.

[10] ISO, "*Information technology – Security techniques – Methodology for IT security evaluation"*, ISO/IEC 18045, current version, International Organization for Standardization.

[11] Norwegian Council for IT Security, *Certification of IT security in products, systems and organisations* (final report), 13 November 1997, (In Norwegian only)

[12] Personal Data Act (2018), *Act No. 38 of 15 June 2018 relating to the processing of personal data*, Ref. https://lovdata.no/dokument/NL/lov/2018-06-15-38

[13] Public Administration Act, *Act of 10 February 1967 relating to procedure in cases related to the public administration*, Ref: https://lovdata.no/dokument/NL/lov/1967-02-10

[14] Regulation relating to public archives*, Regulation No. 2105 of 15 December 2017 relating to public archives*.

[15] Regulation relating to supplemental technical and archive-related provisions relating to the management of public archives, *Regulation No 2286 of* 19 December 2017 *relating to supplemental technical and archive-related provisions relating to the management of public archives* (Director General's regulation of National Archives*)*.

[16] SERTIT (2020), *"Krav til evalueringsfirma – kvalifiseringskrav til evalueringsfirma under den offentlige sertifiseringsordningen for IT-sikkerhet"*, SD 003, version 4.2, 06.04.2020, SERTIT.

[17] SERTIT, *Application for certification*, ST 027E, v. 2.5, SERTIT.

[18] SERTIT (2018)*, "Conditions for use of Certificate and Certifications Mark"*, SD 030E, 3.1, SERTIT.

[19] SERTIT (2017), *Operating Agreement*, SD 006, v. 2.0, SERTIT

[20] SERTIT (2017), *Terms of Reference for SERTIT*, v.1.0, 27.11.2017, SERTIT

[21] Security Act (2018), *Act of national security (Security Act), Act No. 24 of 1 June 2018 relating to national security (Security Act)*, Ref. https:// lovdata.no/dokument/NL/lov/2018-06-01-24.

[22] SOGIS (2019), *Assurance Continuity*, v. 1.0, November 2019, Joint Interpretation Library, SOGIS, Ref.: https://www.sogis.eu/uk/detail_operation_en.html.

[23] SOGIS MRA (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, January 8th 2010.

[24] Standard Norge (2017), *"General requirements for the competence of testing and calibration laboratories"*(ISO/IEC 17025:2017), November 2017, Standard Norge.

[25] Standard Norge (2012), *"Conformity assessment Requirements for bodies certifying products, processes and services"*, (ISO/IEC 17065:2012), September 2012, Standard Norge.

[26] The Protection Instructions, Regulation No. 3352 of 17 March 1972, *Instructions for handling of documents in need of protection for reasons other than those mentioned in the Security Act with regulations*.

Appendix A: History

In autumn 1997 a fact-finding group under the *Norwegian Council for IT Security* prepared a report [11] recommending the establishment of a scheme for certification of IT security in products and systems. The Government decided to establish the Scheme in accordance with the recommendation. Against the background of Proposition No. 1 (1998-99) to the Storting for the Ministry of Trade and Industry, the Storting appropriated funds to the then Headquarters Defence Command Norway/Security Division (CHOD Norway/SEC) for the establishment and operation of SERTIT. Since 1 January 2003 SERTIT has been a part of the Norwegian National Security Authority (NSM).