Guide and checklist for Common Criteria Evaluations

CCLAB

Table of Contents

1 Preamble

The purpose of this document is to briefly summarize the most important steps required to ensure a successful Common Criteria (CC) evaluation (and certification) project based on the Common Criteria evaluation methodology. OCSI/BSI or the given national scheme certifies products and solutions based on the documentation of the evaluation results carried out by CCLab (Test Laboratory). This checklist also documents, that the Developer/Sponsor needs to provide for an evaluation project.

Note

Most of the concepts, procedures, etc. in this document were taken from OCSI (the Italian scheme), therefore they may differ in other schemes, although the basic procedure shall be applied very similarly with each Common Criteria scheme.

Good-to-know before starting the certification process:

TOE (Target of Evaluation): must be decided in advance. The TOE may be an IT product, a part of an IT product, a set of an IT product, a unique technology that may never be made into a product, or a combination of these.

EAL (Evaluation Assurance Level) must be decided before submitting the application to the certification body.

Developer and Sponsor can be the same (Sponsor=who finances the evaluation process)

The TOE (device/product) to be evaluated must be ready before starting an evaluation project for proper project timing. Further development of the TOE during evaluation delays and/or may halt the certification project.

The documentation evaluation precedes the testing of the TOE. Some Evaluation Classes cannot be finalized without providing the TOE for the Test Laboratory.

From the evaluation point of view, the Security Target (ST) has to be ready first. The ST is an implementation-dependent statement of security needs for a specific identified TOE. The ST can be prepared either by the Developer or by an appointed CC Consultant.

A detailed EWP (Evaluation Work Plan) must be prepared by the Test Laboratory and approved by the CB (Certification Body) (see later).

It may be necessary to change some parts of the EWP during the evaluation, for example, in the following cases:

- The TOE is modified during the evaluation (due to a new product version or because some problems have been solved);
- If there are delays on the Developer's side in providing the deliverables and evidences required by the evaluator.

All changes made to an EWP must be approved by the CB.

Evaluation deliverables needed during the evaluation process:

In order to carry out the activities listed in the EWP, the Evaluators must have access to the evaluation materials requested. The evaluation criteria provide a list of evaluation materials for each assurance level (EAL). The Test Laboratory will give a detailed list of the requested materials for each evaluation that will usually be an integral part of the EWP itself.

Evaluation materials, besides the ST, often include:

- Hardware, firmware, or software components that make up the TOE;
- Documentation for TOE users;
- Technical support documentation generated during the TOE development phase or to support the evaluation process;
- Developer technical support documentation.

The following may also be considered evaluation materials (depending, for example, on the chosen EAL (Evaluation Assurance Level)):

- Access to the operational site;
- Access to the TOE development site.

2 Communication

2.1 Before starting the Evaluation:

2.1.1 Preparatory phase

The Sponsor/Developer and CCLab (Test Laboratory) are involved in the preparation phase.

The Test Laboratory analyses the ST to give a Proposal and an estimated timeframe to conduct the evaluation.

Before drawing up a contract /accepting the Proposal, the Sponsor and the Laboratory may choose to contact the Certification Body to ascertain whether the evaluation can be carried out under the chosen scheme or not (the procedure may differ by scheme).

Once the agreement between the Sponsor and the Laboratory has been defined, the Sponsor has to submit a formal request to the Certification Body for the acceptance of the evaluation into the national scheme, accompanied by the ST and the EWP.

2.1.2 Conduct phase

The evaluation starts when the Certification Body, having analysed the materials received, approves the EWP and formally accepts the evaluation into the scheme.

2.2 During the Evaluation:

The following communication means are suggested to ensure a smooth and successful evaluation project:

- Project kick-off meeting between the Laboratory and the Sponsor/Developer - to discuss and agree on the most important milestones, administrative information and operational tasks at the beginning of the project (see below in details)
- Weekly, bi-weekly status meetings - to have a continuous update of the project and have the opportunity to address any arising issues
- Email, secure file exchange (preferably encrypted with PGP keys) - for continuous communication and to share confidential information

3 The conduct phase, i.e. the Evaluation

3.1 Start-up of the evaluation:

- Official kick-off meeting organised by the CB (e.g. OCSI) to discuss the following topics:
- Identification of representatives of both the Sponsor and the Laboratory responsible for the evaluation;
- Identification of members of the certification group designated by the CB;
- Clarification of ST content;
- Clarification of EWP content;
- Handling of confidential documents;
- Management of evaluation materials;
- Details of personnel designated by the Laboratory for the evaluation;
- Evaluation restrictions (such as access limitations for some areas or Developer and/or Sponsor contact restrictions);
- Re-use of previous evaluations' results, if any;
- Requisites and frequency of the Evaluation Review Meetings (if necessary);
- Method of transmission of the documents and materials produced during the evaluation.

3.2 During the Evaluation:

In order to carry out the Evaluation Activities, the Evaluators must have access to the evaluation materials requested.

Postponement of key development milestones or a delay in the issue of an evaluation material will have an impact on evaluation execution timescales.

The Laboratory may, for example:

1. Suspend the action affected and (if applicable) move onto another action;
2. Suspend the whole project until the required material is available (restarting the evaluation may have additional costs to the Sponsor depending on the nature and duration of the delay).

Changes in evaluation execution timescales are governed by a contract between the Laboratory and and the Sponsor, however, these changes may have an impact on the availability of certification resources; therefore, the Laboratory needs to notify the CB of any delays and changes which may affect the critical milestones of the evaluation process.

The non-availability or delay in the issue of evaluation materials, or a found anomaly may result in the issuance of an Observation Report.

The Activity Reports (AR) contain the results of the evaluation carried out according to the CEM of each Class. The results can be: pass, fail, and inconclusive.

The Observation Report contains the "inconclusive" and "fail" work units and an explanatory verdict section, detailing the evaluator's decision.

The ARs are only sent to the CB, while the Observation Reports are sent to the CB and Developer as well.

3.3 Observation Reports (or equivalent)

The Observation Report contains TOE related problems.

Two types of Observation Reports are used:

1. Fault Observation Report (ROE);
2. Anomaly Observation Report (ROA).

3.3.1 Fault Observation Report (ROE)

ROE is produced when an exploitable vulnerability is found during the evaluation, which also contains suggestions about how to correct the found vulnerability.

3.3.2 Anomaly Observation Report (ROA)

An ROA must be used to report all TOE related problems, with the exclusion of exploitable vulnerabilities, such as:

- Problems concerning the development or management of the TOE;
- Problems concerning evaluation evidence content and presentation;
- Problems which may have an impact on security.

ROAs are distributed to the Sponsor and the CB simultaneously, while the ROEs are sent to the CB for review before being delivered to the Sponsor.

3.4 The end of the Evaluation:

The Evaluation Technical Report (ETR) is the final report created by the Laboratory. The ETR contains all the verdicts and considerations made by the Evaluators during the evaluation process. By the time the Laboratory starts creating the ETR, all ARs must be finalised, i.e., the verdict of all work units must be a "Pass". The ETR is sent exclusively to the CB for review to ascertain that an adequate summary of the evaluation results are provided. This is the basis for the Certification Report of the TOE.

3.5 Certification Report:

Thirty days[1] from the approval of the ETR the CB draws up a draft Certification Report (CR) that is sent to the Laboratory and Sponsor to obtain confirmation that it does not contain clerical errors and/or pieces of confidential information. The Laboratory and the Sponsor respond to the request within the next five working days.

Once the CB has received confirmation from the Laboratory and Sponsor, or response deadline has passed, the CB issues the Certification Report within thirty days.

In the Certification Report the CB:

a. Declares if the evaluation has been carried out using the criteria and methodology prescribed by the national scheme;

b. Declares whether the Security Target is complete, appropriate and technically sound;

c. Declares whether the Target of Evaluation satisfies the Security Target for the level of assurance requested;

d. Identifies any residual vulnerabilities and possibly recommend countermeasures;

3.6 Certificate issuance:

Upon successful evaluation, the CB adds the Certificate to the CR, which is the declaration that the TOE has been evaluated by an accredited Laboratory according to the evaluation criteria and the Scheme procedures. **The issued Common Criteria Certificate only applies to the specific version of the TOE in its evaluated configuration and declares that the level of assurance requested has been achieved. The final certificate will be listed on commoncriteriaportal.org** and the CB's website.

4 References

Terms, Definitions and Abbreviations used but not defined in here can be found in the following documents:

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

Note: For up-to-date documents please always visit: Common Criteria Portal

1 Procedural time may differ by scheme. OCSI works with a 30 days deadline.

A COMPLETE PROCESS OF A COMMON CRITERIA EVALUATION PROJECT