Combitech EUCC Certification and Evaluation Scheme (External version)

Contents

1 Introduction

The document “Combitech EUCC Certification and Evaluation Scheme” is the top document of the Combitech certification and evaluation regulations for use with EUCC, defined by its implementing act, *Commission Implementing Regulation (EU) 2024/482 of 31.1.2024*, ref. [22] and its amendments in ref. [24]. EUCC and Combitech’s certification and evaluation regulations are below called the Combitech EUCC Certification and Evaluation Scheme or just the Scheme. This version is the external version of the Scheme, a summarized version of the complete Scheme [27].

This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of Information and Communications Technology (ICT) products for which security is a consideration, as well as those already involved with the Scheme, e.g., certifiers, evaluators, customers, contractors, and security consultants.

1.1 Terminology

The following terms are used to specify requirements:

SHALL — Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).

SHOULD — Within normative text, “SHOULD” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

MAY — Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).

CAN — Within normative text, “CAN” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).

2 Overview

Combitech is acting as Conformity Assessment Body (CAB) under the Cybersecurity Act (CSA), ref. [25], with a Certification Center (CB) and an IT Security Evaluation Facility (ITSEF). The CB is below called Certification Center or CB and the ITSEF is called Evaluation Center or ITSEF.

Combitech CAB is operating under the EUCC scheme at assurance level Substantial, AVA_VAN.2 and High, AVA_VAN.3, for specified product categories.

After a successful evaluation and certification, the Certification Center will issue an EUCC certificate.

After a per-certificate oversight process responsible by the Swedish NCCA, certificates may be recognized up to the level of EAL2 by the member states of the Common Criteria Recognition Arrangement, CCRA, ref. [26].The process of evaluation and certification involves the following parties with specific responsibilities, which are detailed in chapter 0,

Roles and Responsibilities.

- Sponsor
- Developer
- ITSEF
- Certification Center

This leads to the structure depicted in Figure 1 of the different parties currently involved in the Combitech EUCC Certification and Evaluation Scheme implementation.

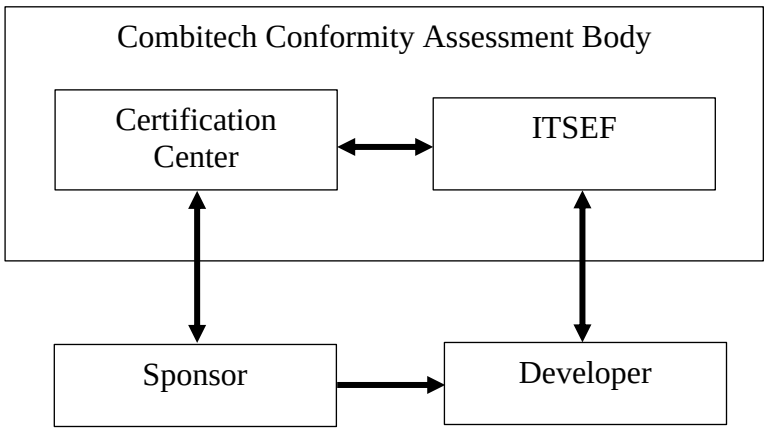

Figure 1, Combitech EUCC scheme implementation

3 Legislation and Standards

3.1 Cybersecurity Act

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, ref. [25]

3.2 EUCC Implementing Regulation

Commission Implementing Regulation (EU) 2024/482 of 31.1.2024, ref. [22]
Annexes to the Commission Implementing Regulation, ref. [23]
Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation, ref. [24].

3.3 Standards

CCMB-2017-04-01, Common Criteria version 3.1 revision 5, part 1, ref. [1]

CCMB-2017-04-02, Common Criteria version 3.1 revision 5, part 2, ref. [2]

CCMB-2017-04-03, Common Criteria version 3.1 revision 5, part 3, ref. [3]

CCMB-2017-04-04, Common Criteria version 3.1 revision 5, evaluation methodology, ref. [4]

CCMB-2022-11-001, Common Criteria version CC:2022 revision 1, part 1, ref. [5]

CCMB-2022-11-002, Common Criteria version CC:2022 revision 1, part 2, ref. [6]

CCMB-2022-11-003, Common Criteria version CC:2022 revision 1, part 3, ref. [7]

CCMB-2022-11-004, Common Criteria version CC:2022 revision 1, part 4, ref. [8]

CCMB-2022-11-005, Common Criteria version CC:2022 revision 1, part 5, ref. [9]

ISO/IEC 15408-1, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 1, ref. [10]

ISO/IEC 15408-2, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 2, ref. [11]

ISO/IEC 15408-3, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 3, ref. [12]

ISO/IEC 15408-4, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 4, ref. [13]

ISO/IEC 15408-5, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 5, ref. [14]

ISO/IEC 18045, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, third edition, 2022-08 - Methodology for IT security evaluation, ref. [15]

ISO/IEC TR 22216, Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022, ref. [16].

ISO/IEC 17025:2018, General requirements for the competence of testing and calibration laboratories, 2018-05-07, ref. [17]

ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services, 2012-09-15, ref. [18]

3.4 Accreditation regulations

STAFS 2020:1, Styrelsen för ackreditering och teknisk kontrolls föreskrifter och allmänna råd om ackreditering, 2020-04-29, ref. [19].

3.5 Common Criteria Recognition Arrangement

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, CCRA, July 2, 2014, ref. [26].

4 Types of Certifications

Combitech EUCC CAB performs evaluation and certification of Information and Communication Technologies (ICT) products as defined by the CSA and EUCC as well as Protection Profiles (PP) as CC technical specifications.

5 Roles and Responsibilities

5.1 Sponsor

The Sponsor is the organization that funds the evaluation and certification, applies to the Certification Center for certification, contracts with the ITSEF, and arranges for Developer participation. The Sponsor and the Developer may be the same.

The Sponsor SHALL have formal agreements with the Certification Center for the certification.

The Sponsor SHALL ensure that evaluation evidence, training, support, and access to facilities is provided to the Evaluator. This MAY require an agreement with the Developer, as well.

The Sponsor SHALL ensure that the Certifier is provided with evaluation evidence, training, support, and access to facilities if required by the Certifier.

The Sponsor SHALL assign a point of contact for the evaluation and certification, which is the contact person to use for the other parties involved. This point of contact SHOULD be the recipient for all communication with the Sponsor within the scope of the evaluation and certification, including business correspondence, the certification report, and the certificate. The Sponsor SHALL ensure that the Certification Center is notified of any changes to the point of contact.

Upon successful certification, the Sponsor is responsible for archiving a reference copy of the target of evaluation as well as any and all evidence produced by the Sponsor or the Developer that has been used by the Evaluator or by the Certification Center to perform evaluation or certification activities.

The archived material SHALL be complete in order to enable the course of the evaluation and certification to be traced and re-confirmed. It SHALL be securely and accessibly archived for at least five years from the date at which the certificate is issued.

The archived material SHALL be made available to Certification Center at request within seven working days.

The Sponsor, as the holder of the certificate, SHOULD, during the validity period of the certificate, monitor detection of potential non-compliance issues which affect a certified ICT product. The Sponsor SHOULD follow the process described in section 11.5.3 *Compliance Monitoring* upon such detection.

5.2 Developer

The Developer is the organization that produces the target of evaluation. The Developer supports the Sponsor during the evaluation by providing necessary documentation, technical know-how, and evaluation evidence to the Evaluator. The Developer and the Sponsor may be the same organization.

All Developer requirements are in legal terms, requirements on the Sponsor with whom the Certification Center has an agreement. In practice, the Developer is the party who will need to take action to fulfil these requirements.

The Developer SHALL:

- assign a technical point of contact who the other parties can contact for target of evaluation support and clarifications;
- support the evaluation, for example, by educating Evaluators and Certifiers on the target of evaluation;
- develop and deliver evaluation evidence;
- respond to Evaluator and Certifier findings, for example, by updating or producing new evaluation evidence; and
- support the Evaluator during site visits, for example, by ensuring that the Evaluator has access to development areas and can interview key personnel.

If the Developer is distinct from the Sponsor, it may be necessary that the Developer and the Sponsor agree how to support the evaluation.

5.3 ITSEF

The ITSEF is the organization that performs the evaluation. It is responsible for ensuring that the assessment performed is consistent with the CC, the CEM, and the Scheme.

The ITSEF is subject to supervision by both the Certification Center and the accreditation body as appropriate to ensure that it meets its obligations.

The ITSEF's Evaluator performs the assessment of the target of evaluation. The Evaluator provides the Certification Center with evaluation reports containing findings and verdicts, such as observation reports, single evaluation reports, and final evaluation reports.

5.4 Certification Center

The Certification Center provides independent confirmation of the evaluation results by overseeing the evaluation process. The Certification Center SHALL carry out surveillance of the ITSEF operation through its day-to-day involvement in the evaluations performed by the ITSEF.

The Certifier oversees an evaluation by reviewing the evaluation reports produced by the Evaluator. The result is documented in evaluation oversight reports.

Witnessing the Evaluator's site visits at the Developer site is added for EAL 3 or higher, unless otherwise decided. The Certifier may also witness the testing of the target of evaluation.

6 Changes Affecting the Certification/Evaluation

Any changes in the requirements, new or revised, that affect a client SHALL be communicated to all affected clients in writing.

Any changes to an agreed certification and evaluation process, proposed by either the Sponsor or the Certification Center, SHALL be considered by the parties and, if agreed, documented in the SoW and/or PO.

7 Confidential Information Management

7.1 Confidentiality Claims and Protective Marking

Originators of information SHALL make the Certification Center aware of any confidentiality claims regarding information that is shared with the Certification Center.

Documents with confidentiality claims regarding the entire document or parts thereof SHOULD bear protective marks indicating that the information should be regarded as confidential. The originator MAY otherwise inform, verbally or in writing, the confidentiality status claimed for a document or parts of it.

If the identity of a party (Sponsor, Developer, etc.) or the target of evaluation is to be treated as confidential this SHALL be clarified in the certification application.

7.2 Protection of Confidential Information

The Certification Center SHALL treat confidential information as it treats its own Company Confidential information. That is, only store and internally communicate the confidential information in the company internal network or in a secured enclosure.

Measures for external communication of confidential information shall be agreed by the originator and the Certification Center.

When the Certification Center is required by law or authorized by contractual arrangements to release confidential information, the originator concerned shall, unless prohibited by law, be notified of the information provided.

8 Records

The Certification Center SHALL retain records to demonstrate that all certification and evaluation process requirements have been effectively fulfilled as long as the certificate is valid, and at least five years after the withdrawal of the certificate.

The records shall be treated confidentially as described in section 7.2 *Protection of Confidential Information.*

The Sponsor undertakes to keep records of the information provided to the Certification Center and to the ITSEF during the certification process and at least five years after the withdrawal of the certificate. Upon request by the Certification Center or the Swedish NCCA the holder of a certificate shall make available the records.

9 Conditions for Use of Certificates and Trademarks

The rules for use of certificates and trademarks are described in the scheme document Combitech EUCC Use of Trademarks, [20].

10 Impartiality Assessment

The Combitech Certification and Evaluation Scheme may have stakeholders from all over the world. Therefore, physically nor digitally meetings are not suitable as the required impartiality assessment mechanism. The impartiality assessment is instead performed using digital communication mechanisms, such as mail, web forms, or similar.

The interested parties are informed in writing about the Scheme organization, operation and performance as well as any complaints or appeals received since the previous assessment. The interested parties are asked to provide their input about the impartiality of the Scheme.

The Head of the Certification Center is obligated to take action in due time, however, within 30 days at the latest, if any impartiality issues are raised.

The impartiality assessment is performed every 18 month and the invited significantly interested parties includes, but are not restricted to:

a) Customers
b) FMV CSEC
c) Combitech

The following topics are subject to review:

- Approval of the report from last review
- Matters concerning invited parties
- Emphasis on the invited parties to ensure the impartiality of the operations of the Certification Center and the members right to take actions when advice is not followed
- Report from activities by the Combitech Conformity Assessment Body, CAB, since last review
- Changes to the Scheme
- Proposed changes to the Scheme
- Report from risk analysis
- Combitech CAB matters regarding:
    - ITSEF and evaluator qualifications
    - Evaluation
    - Certification
    - Customer Satisfaction
    - Complaints
    - Appeals
    - Feedback from interested parties
- News and status regarding
    - Common Criteria
    - EUCC
    - CCRA
- Conclusion - Any matters that indicate that the Certification Center do not act impartial
- Proposed date for the next meeting

Input from the invited parties is compiled and distributed as a report to all invited parties together with Combitech CAB’s response and plan for possible corrective actions, if needed.

11 Scheme Processes

11.1 Certification Agreement

Combitech Certification Center signs a legally enforceable agreement for the provision of certification and evaluation activities with its clients.

This agreement is established as follows.

1. The Sponsor contacts the Certification Center and declare its interest for evaluation and certification of an ICT product. The Certification Center can be contacted orally, by mail, by a web-based Application Form, or otherwise.

2. The Certification Center ensures that all information necessary for the evaluation and certification process is provided by the Sponsor[1]. This includes, but is not limited to:

    - The product name, version, and type;
    - The standard to be used, assurance level, and/or claimed Protection Profile;
    - A description of the product necessary to get an understanding of the complexity, scope, and security functionality of the product. Preferably, a draft Security Target is used.
    - All necessary information about the Sponsor and the Developer, such as company/organization name, address, legally status, point of contact, contact information, billing address.
    - The status of the product and a suggested time frame for the evaluation and certification.
    - A description of the Sponsor/developer’s vulnerability management and vulnerability disclosure procedures.

3. The Certification Center judges that

    - all prerequisites are met;
    - all means for the evaluation and certification activities are available;
    - the Certification Center and the ITSEF have the competence and capability to perform the evaluation and certification activities; and
    - the Certification Center and the ITSEF have enough personnel resources available that comply to the impartiality rules.

[1] The information may be obtained from appropriate evaluation results from prior certification.

4. The Certification Center and the Sponsor agrees on and mutually signs a Statement of Work (SOW) stating the terms and fees for the services.

5. The Sponsor sends a Purchase Order (PO) referring to the SOW to the Certification Center.

6. The Certification Center accepts the purchase order.

7. An Evaluation Work Plan, EWP, is mutually developed by the Sponsor/Developer, the Certification Center and the ITSEF.

The Certification Center shall inform the client of any activity of its legal entity including being a designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product that might be related to the type of products of the client.

The Certification Center shall inform the client of its obligations to allow assessment teams from Swedac and/or EA, IAF, ILAC to witness the Combitech Certification Center's work at the premises of the client and/or its subcontractors.

The accepted SOW and PO together form the Certification Agreement. The Certification Agreement SHALL state that the requirements and regulations of the Scheme SHALL be met.

If the Certification Center judges that it lacks enough competence or capability for the evaluation and certification activities it is required to undertake and the missing competence or capability is not possible to achieve by supporting external experts, it will decline the requested services.

11.2 Evaluation and Certification

The evaluation and certification are performed in separate phases including:

d) Planning;
e) Evaluation;
f) Certification; and
g) Conclusion.

11.2.1 Planning Phase

Before the product evaluation begins the Sponsor/Developer, the ITSEF and the Certification Center plans their resources and deliveries.

The ITSEF and Certification Center plan their evaluation respectively certification teams, the locations, the test and IT systems to be used, etc.

Impartiality declarations are documented for all personnel involved in the evaluation and certification; even external experts used as support. In case of staff changes during the evaluation and certification process, impartiality declarations shall be documented for the new team members.

The Certification Center shall, if needed, inform the Sponsor/Developer of the details in the evaluation and certification process, required deliveries, etc., that have not already been agreed in the SoW.

The Sponsor/Developer and the Certification Center/ITSEF shall agree on arrangements for mutual activities such as testing and site visit at Developer premises, if required.

All parties shall also agree on the means for secure communication of information and the language used in the documentation.

11.2.2 Evaluation Phase

The Evaluation Phase includes the following steps:

1. The Developer delivers evaluation evidence according to the Common Criteria requirements to the Evaluator.

2. The Evaluator reviews the evaluation evidence for each Common Criteria Class and document the review, potential findings, and verdicts in a separate Single Evaluation Report, SER, for each Class.

3. Potential findings are documented and presented for the Developer in an Observation Report, OR.

4. The Developer responds to the OR with updated evidence and or clarifications to the Evaluator

5. The Evaluator accepts the Developer’s response or the steps 3 and 4 are iterated.

6. When all findings in an OR are solved, the corresponding SER is finalized and submitted together with the OR to the Certifier.

7. The Certifier review the SER and OR and submit a Certifier Oversight Report (COR) to the Evaluator. Any potential comments in the CER are handled by the Evaluator either by updating the SER or by performing step 3 again.

8. When all findings for all Classes are solved, the Evaluator summarizes the evaluation in a Final Evaluation Report (FER). The FER is submitted to the Certifier.

9. The Evaluation Phase is finished and the Certification Phase begins.

Evaluation of the ALC Class, above Evaluation Assurance Level 2 (EAL2) includes also that the Evaluator performs site visit according to the methodology in CEM, ref. [4], at the site/sites the Target of Evaluation (TOE) is/are developed. Potential findings are handled as in step 3 and forward.

Evaluation of the ATE and AVA Classes includes also that the Evaluator performs independent and vulnerability testing. Potential findings are handled as in step 3 and forward.

The Common Criteria Class ASE, Security Target, has to be evaluated first, the other Classes are preferrable evaluated in the order depicted in Figure 2, from top and downwards. If findings later in the process is found for a Class already evaluated, the verdict for that Class may be changed and the findings may be handled as in step 3 and forward.

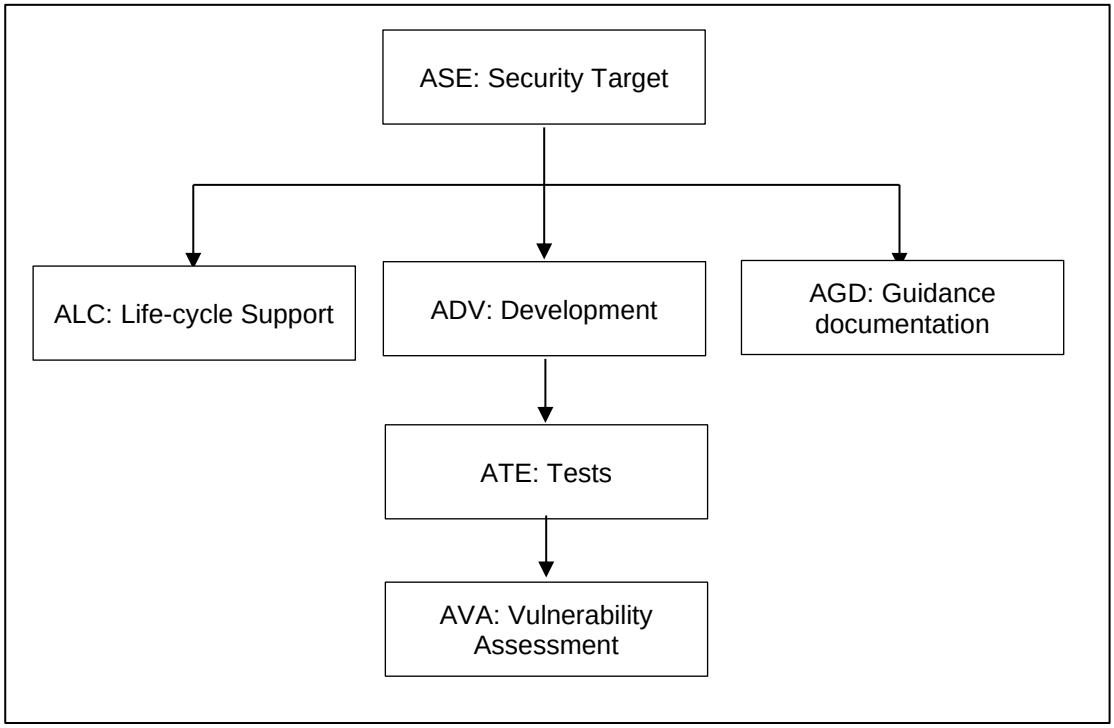

Figure 2, Evaluation order

11.2.3 Certification Phase

In the Certification Phase the evaluation is finished. The Certifier reviews the FER and ask the Evaluator to correct potential errors.

The Quality Manager of the Certification Center shall have access to the documentation produced and evidence collected during the evaluation and certification to be able to assess that the Scheme rules and the base for accreditation have been followed.

The Head of the Certification Center takes the final certification decision based on the recommendation from the Certifier and Quality Manager. The Head of the Certification Center shall have access to the documentation produced and evidence collected during the evaluation and certification to be able to assess the verdicts.

The Certifier produces a Certification Report (CR), mainly based on the FER, and the Certificate(s). The CR and Certificate(s) shall be published together with the final Security Target and the Sponsor, Developer, and Evaluator are offered opportunity to review the CR and the Certificate(s).

When no more comments on the CR nor Certificate(s) remain, the CR, Certificate(s), and Security Target are published at Combitech's and Enisa's web-sites.

11.2.4 Conclusion Phase

After the evaluation has been finished, the Evaluator SHALL handle all material used during the evaluation according to the terms in the evaluation agreement; material will be archived, returned, or destroyed, as agreed.

The Certification Center SHALL archive the reference material needed to demonstrate the certification results and how the certification was performed.

11.3 Assurance Continuity

Assurance continuity SHALL be performed according to Annex IV, *EUCC Annexes to the Commission Implementing Regulation*, ref. [23].

The Sponsor may request assurance continuity if a certificate is due to expire within nine months or if the certified product has been changed or if there are demands that the vulnerability assessment is carried out again.

The assurance continuity process within the Scheme is described below.

11.3.1 Assurance Continuity Agreement

Combitech Certification Center signs a legally enforceable agreement for the provision of assurance continuity activities with its clients.

This agreement is established as follows.

1. The Sponsor contacts the Certification Center and declare its interest for assurance continuity of an ICT product certified by the Certification Center. The Certification Center can be contacted orally, by mail, by a web-based Application Form, or otherwise.

2. The Certification Center ensures that all information necessary for the assurance continuity process is provided by the Sponsor. This includes, but is not limited to:

    - The Certification Id of the previously certified ICT product;
    - The certified Security Target;
    - The reason for the Assurance Continuity. The reason could be:
        - Changes in the certified TOE;
        - Changes in the certified TOE developing environment;
        - Changes in the certified TOE operating environment;
        - Changes in the certified TOE threat environment;
        - Changes in the ICT product not concerning the TOE functionality;
        - The TOE certificate is near its expiration date;
        - Required by the certified patch management procedure for the TOE;
        - Required by the compliance monitoring process;
        - Other reasons.
    - Description of changes in the TOE, the TOE operating environment, the TOE developing environment and/or the TOE threat environment;
    - Any changes of the necessary information about the Sponsor and the Developer, such as company/organization name, address, legally status, point of contact, contact information, billing address.

3. The Certification Center engages the ITSEF with the information stated in step 2. The ITSEF may request complementary information from the Developer.

4. The ITSEF produces an Impact Analysis Report, IAR, including an assessment of the changes resulting in a conclusion if the they are minor or major. Minor changes could be:
    - None-security related bug fix in the TOE;
    - Some changes in the certified TOE developing environment;
    - Changes in the ICT product not concerning the TOE functionality; or
    - Likewise.

    Major changes could be:
    - Security related bug fix in the TOE;
    - Changes in the certified TOE threat environment; or
    - Likewise;

    Note that change of security related functionality that affects the Security Target always will require a new evaluation and certification.

5. The Certification Center review the IAR to confirm that it is complete, consistent, and sound. If the Certification Center judges that

    - all prerequisites are met;
    - all means for the assurance continuity activities are available;
    - the Certification Center and the ITSEF have the competence and capability to perform the assurance continuity activities; and
    - the Certification Center and the ITSEF have enough personnel resources available that comply to the impartiality rules.

6. The Certification Center and the Sponsor agrees on and mutually signs a Statement of Work (SOW) stating the terms and fees for the services.
7. The Sponsor sends a Purchase Order (PO) referring to the SOW to the Certification Center.
8. The Certification Center accepts the purchase order.

The accepted SOW and PO together form the Assurance Continuity Agreement. The Assurance Continuity Agreement SHALL state that the requirements and regulations of the Scheme SHALL be met.

If the Certification Center judges that it lacks enough competence or capability for the assurance continuity activities it is required to undertake and the missing competence or capability is not possible to achieve by supporting external experts, it will decline the requested services.

Depending on if the changes is deemed to be minor or major, either the Certificate Maintenance or the Re-evaluation processes

11.3.2 Certificate Maintenance

When the changes have been classified as minor, the procedure described in Annex IV, *EUCC Annexes to the Commission Implementing Regulation*, ref. [23], IV:3 *Changes to a certified ICT product* paragraph 5 - 6 SHALL be applied.

11.3.3 Re-evaluation

When the changes have been classified as major, the procedure described in Annex IV, *EUCC Annexes to the Commission Implementing Regulation*, ref. [23], IV:3 *Changes to a certified ICT product* paragraph 7 - 9 SHALL be applied.

11.4 Patch Management

If the Sponsor/Developer has developed a software or hardware patch according to their ALC_FLR, [CC 2022 p3] patch management procedure and want to apply the patch to the certified product, they shall take the following steps within 5 working days.

a) If the functionalities affected by the patch reside outside the target of evaluation of the certified product:

- Report the patch to CB Certification Center. The concerned certificate will not be changed.

b) the patch relates to a predetermined minor change to the certified ICT product;

- Submit the patch to the ITSEF. The ITSEF shall inform CB Certification Center after the reception of the patch upon which CB Certification Center takes the appropriate action on the issuance of a new version of the corresponding EUCC certificate and the update of the certification report;

c) the patch relates to a confirmed vulnerability with critical effects on the security of the certified ICT product.

- Submit the patch to the ITSEF for the necessary re-evaluation but may deploy the patch in parallel. The ITSEF shall inform CB Certification Center after which it starts the related applicable certification activities according to section 11.3.3 *Re-evaluation*.

11.5 Certificate Validity

11.5.1 Valid Certificates

An ICT product certificate SHOULD be valid for five (5) years. Certificate validity could be extended according the Assurance Continuity procedures described in section 11.3 *Assurance Continuity.* Certificate validity could also be shortened according to the Compliance Monitoring procedures described in section 11.5.3 *Compliance Monitoring.*

11.5.2 Expired Certificates

Certificates with an expired validity period SHALL be archived and made available by:

- ENISA in a different webpage than the valid ones on European cybersecurity certification schemes;
- Combitech in the list of Archived certificates on the Combitech EUCC website; and
- NCCA on <TBD>.

11.5.3 Compliance Monitoring

The Sponsor of a certificate SHOULD monitor detection of potential non-compliance issues which may affect the certified ICT product.

Potential non-compliance issues may also be detected by the Certification Center or detected and reported by customers of the certified product, researchers, or other market surveillance authorities. The Sponsor shall in these cases be notified of the non-compliance issue by the Certification Center.

11.5.3.1 Vulnerability Detection

Upon detection of vulnerabilities within a certified ICT product, the following steps SHOULD be performed.

1. The Sponsor performs a vulnerability impact analysis of the potential non-compliance issue. If the vulnerability impact analysis confirms that the vulnerability can be exploited a report of the assessment should and presents the report to the Certification Center. The assessment report SHOULD include:

    - A description of the vulnerability and how it was detected. If applicable, a reference to a vulnerability database such as CVE, NVD, or likewise.

    - Where applicable, an attack potential calculation shall be performed in accordance with the CEM, ref. [4].

    - A description of the possible impact the vulnerability may have on the certified ICT product, if exploited, and possible risks associated with the proximity or availability of an attack.

    - A description of measures, if any, already taken or planned by the Sponsor/Developer to diminish the effect, mitigate, or remedy the vulnerability.

2. The Certification Center informs the Swedish NCCA of the vulnerability.

3. If no measures have been taken or planned according to step 1 at the time for the vulnerability impact analysis submission to the Certification Center, the Sponsor may within a time frame of maximum 30 days propose such measures.

4. The Certification Center estimates the emergency the vulnerability cause and decides if a suspension or withdrawal of the certificate is necessary.

11.5.3.2 Other Non-compliance

If the obligations of the Sponsor/Developer under EU Cybersecurity Act, ref. [25], or EUCC, ref. [22], ref. [24], towards the EUCC certificate that was issued by the Certification Center are not fulfilled, the Certification Center estimates the emergency of the non-compliance and decides if a suspension or withdrawal of the certificate is necessary. The Certification Center shall inform the Swedish NCCA of the non-compliance.

An example of non-compliance is if the Sponsor/Developer cease to exists and cannot fulfill their monitoring obligations during the validity time of the certificate. The Sponsor may by other reasons request the certificate to be withdrawn.

In case of non-compliance by the Certification Center or ITSEF, identified by the Swedish NCCA, each affected certificate issued by the Certification Center shall either be maintained unaltered or withdrawn after decision by the Certification Center.

11.5.3.3 Suspension and Withdrawal

If the Certification Center decides to suspend a certificate the suspension period starts the day after the decision is made and lasts no longer than 42 days.

The Sponsor and the Swedish NCCA are informed about the decision and the reasons immediately. The Sponsor is informed that the certificate customers shall be informed about the suspension, the reasons and possible security risks.

ENISA shall be informed about suspensions and withdrawals.

Upon withdrawal of a certificate, the Sponsor shall disclose and register any publicly known and remediated vulnerability in the ICT product on the European vulnerability database.

11.6 Complaints and Appeals

11.6.1 Complaints

The Certification Center SHALL document and investigate any complaint directed towards it that applies to the certification activities for which it is responsible. All such complaints will be registered be handled according to the procedures described in the internal Quality Management System.

The Certification Center SHALL:

1. Confirm whether the complaint relates to the certification activities;
2. Inform the complainant that the complaint has been received and that it will be treated as a complaint;
3. Document and record the complaint for further handling;
4. Investigate the complaint and if necessary, seeking the aid of impartial and independent technical experts;
5. Determine whether the decision made or action performed causing the complaint has been made on false grounds, in conflict with the scheme regulations (ISO/IEC 17065:2012, CC, CEM, scheme specific documents), or for any other reason is found to be incorrect;
6. Establish a plan for implementation of corrective actions, the plan may involve compliance monitoring activities according to section 11.5.3 Compliance Monitoring;
7. Execute the plan according to the normal procedures for improvements and management of deviations and deficiencies;
8. Document the corrective actions taken;

9. The complainant is informed about the outcome of the complaint;
10. The complainant is of his/her right to appeal;

Forms for complaints can be found on the Combitech website: TBD. The use of these forms is not mandatory.

11.6.2 Appeals

A complainant that is not satisfied with a decision, or with the outcome of a complaint, that applies to the certification activities for which the Certification Center is responsible may file an appeal.

The appeal shall be made within 30 days of the original decision, it shall be made in writing, and it shall contain the following information:

- the decision that is appealed;
- the requested change; and
- the name, address, and telephone number of the appellant.

To preserve the impartiality of the appeals process, appeals are handled by personnel not involved in the decision appealed.

The Certification Center SHALL:

- Confirm whether the appeal relates to the certification activities;
- Document the appeal;
- Check that the appeal has arrived in time and contains all necessary information;
- Inform the appellant that the appeal has been received and that it will be treated as an appeal;
- Investigate and handle the appeal, and proposing consequent actions (if necessary, the aid of impartial and independent technical experts shall be used);
- Determine whether the decision under investigation has been made on false grounds, in conflict with ISO/IEC 17065:2012, CC, CEM, and/or the Quality Management System, or if it contains errors; and
- Decide about the appeal; and
- Ensure that the appellant is informed about the outcome of the appeal.

The Head of the Certification Center has the authority to take the final decision whether to accept or decline the appeal.

12 References

[1] CCMB-2017-04-01, Common Criteria version 3.1 revision 5, part 1

[2] CCMB-2017-04-02, Common Criteria version 3.1 revision 5, part 2

[3] CCMB-2017-04-03, Common Criteria version 3.1 revision 5, part 3

[4] CCMB-2017-04-04, Common Criteria version 3.1 revision 5, evaluation methodology

[5] CCMB-2022-11-001, Common Criteria version CC:2022 revision 1, part 1

[6] CCMB-2022-11-002, Common Criteria version CC:2022 revision 1, part 2

[7] CCMB-2022-11-003, Common Criteria version CC:2022 revision 1, part 3

[8] CCMB-2022-11-004, Common Criteria version CC:2022 revision 1, part 4

[9] CCMB-2022-11-005, Common Criteria version CC:2022 revision 1, part 5

[10] ISO/IEC 15408-1, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 1

[11] ISO/IEC 15408-2, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 2

[12] ISO/IEC 15408-3, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 3

[13] ISO/IEC 15408-4, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 4

[14] ISO/IEC 15408-5, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 5

[15] ISO/IEC 18045, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, third edition, 2022-08 - Methodology for IT security evaluation

[16] ISO/IEC TR 22216, Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

[17] ISO/IEC 17025:2018, General requirements for the competence of testing and calibration laboratories, 2018-05-07

[18] ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services, 2012-09-15

[19] STAFS 2020:1, Styrelsen för ackreditering och teknisk kontrolls föreskrifter och allmänna råd om ackreditering, 2020-04-29

[20] Combitech EUCC Use of Trademarks, version 1.0, CAB-240704-113629-541, Combitech AB

[21] Combitech EUCC Statement of Work, template. Version 1.0, Combitech AB

[22] Commission Implementing Regulation (EU) 2024/482 of 31.1.2024

[23] Annexes to the Commission Implementing Regulation, 31.1.2024

[24] Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

[25] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019

[26] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, CCRA, July 2, 2014

[27] Combitech EUCC Certification and Evaluation Scheme, 2025-05-21, Issue 1.4, CAB-240701-164858-361:004