Swedish Certification Body for IT Security

301 Certification and Evaluation - EUCC - Overview

Issue: 1.0, 2021-Nov-03

Authorisation: Mats Engquist, Acting Head of CSEC , CSEC

Table of Contents

1 Preface

1 This document contains a general description of certification and evaluation under the EUCC scheme. It is the public top document of the CSEC EUCC certification regulations.

2 This document is part of a series of documents that provide a description of aspects of the CSEC EUCC and procedures applied under it. This document is of value to all participants under the CSEC EUCC, 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 Certification Body i.e. employees at the Certification Body, Evaluators, current customers, contractors, and security consultants.

3 The CSEC EUCC documents and further information can be obtained from the Swedish Certification Body for IT Security. Complete contact information is provided in the following box.

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62

Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

4 This document provides a general overview of the CSEC EUCC. It is intended for any party interested in the CSEC EUCC, including developers, customers, and users of ICT security products.

5 Detailed information on specific aspects of the CSEC EUCC is provided in other documents in the series of External publications published by CSEC.

1.2 Terminology

6 Abbreviations commonly used by the Swedish Certification Body for IT Security (CSEC) in External Publications (EP) are for all EP-documents described in Appendix A in this document, EP-301 *Certification and Evaluation - EUCC - Overview.*

7 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 Introduction

2.1 Overview

8 CSEC is an entity within the Swedish Defence Materiel Administration (FMV) acting as Certification Body (CB) and conformance assessment body (CAB) within the Cybersecurity Act (CSA). The CSEC EUCC is operating under the EUCC scheme.

9 The CSEC EUCC operates on assurance level *high* of the CSA.

10 This includes the following types of certifications:

- AVA_VAN.3
- AVA_VAN.4 and AVA_VAN.5 based on a Protection Profile laid down in Annex 16 of [ENISA]

11 The Technical Domains *smart cards and similar devices* and *hardware devices with security box* as defined by [ENISA] are not covered by CSEC EUCC.

12 After a successful evaluation and certification the Certification Body will issue a EUCC certificate.

2.2 Brief Description of CSEC EUCC

13 The cornerstone of the CSEC EUCC is the process of evaluation and certification, whereby security evaluations are carried out by licensed IT Security Evaluation Facilities (ITSEF) and certifications are carried out by the Certification Body.

14 Evaluation is the assessment of an ICT product or a protection profile (PP) against the CC using the Common Methodology for Information Technology Evaluation (CEM) to determine whether or not the security claims on the product or protection profile are justified.

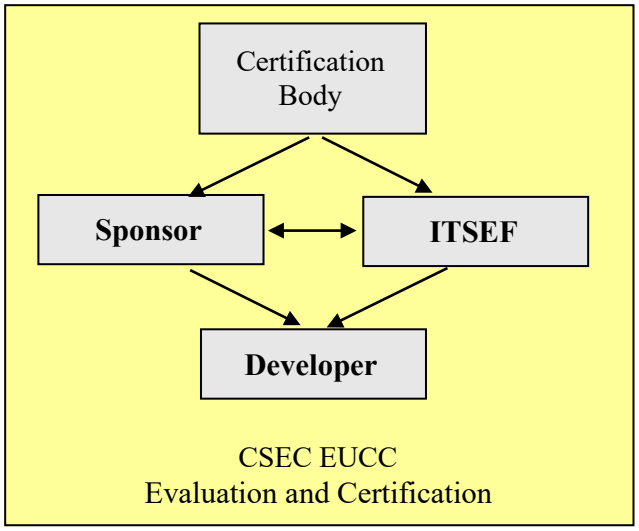
15 Certification is the process carried out by the Certification Body leading to the issuing of a CC certificate. The certificate is a public document issued by the Certification Body which confirms that a specific ICT product or protection profile has successfully completed evaluation by an ITSEF. A EUCC certificate always has a certification report associated with it.

16 The process of evaluation and certification involves the following parties with specific responsibilities, which are detailed in section 4, Roles within CSEC EUCC.

- Sponsor
- Developer
- ITSEF
- Certification Body

17 This leads to the structure depicted in Figure 1 of the different parties currently involved in the CSEC EUCC.

Figure 1 – Organisational Structure of the CSEC EUCC



18 For the evaluation and certification process to work, the framework provided by the CSEC EUCC must define additional processes, which are necessary to set up the organisational context and to achieve recognition of the certificates issued.

19 Additional processes and procedures are:

- Compliance monitoring
- Assurance continuity
- Licensing of Evaluation Facilities
- Interpretations
- Complaints and Appeals

20 These processes are explained in section 5, Processes within the CSEC EUCC , and detailed in additional documents (see section 2.6, Documentation).

2.3 EUCC scheme

The EUCC scheme is owned by the EU Commission. This scheme is established by the implementation regulation.

21 *The COMMISSION IMPLEMENTING REGULATION (EU) …/... of XXX establishing the Common Criteria-based European cybersecurity certification scheme (EUCC)* is owned by the EU Commission.

2.4 Relevant Legislation, Standards and Regulations

2.4.1 Cybersecurity Act

22 REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

2.4.2 Commission implementing regulation

23 COMMISSION IMPLEMENTING REGULATION (EU) …/... of XXX establishing the Common Criteria-based European cybersecurity certification scheme (EUCC)

2.4.3 Government Ordinance

24 In the *Ordinance with Supplementary Directions to the EU Cybersecurity Act* (SFS 2021:555), the Swedish Government has stated that FMV is the Swedish authority for cybersecurity certification, and that at FMV there is an accredited conformity assessment body according to Article 60.2 of the Cybersecurity Act.

2.4.4 Standards

25 The EUCC relies on a set of international standards to support the objectives set forth in this document.

Common Criteria (CC)

26 First and foremost, the CC is the standard that defines IT security evaluation, with the related CEM defining the methodology for evaluators to perform their work. Where questions have arisen about the intent of specific clauses of the CC or the CEM, interpretations have been issued by the Common Criteria Maintenance Board (CCMB).

ISO/IEC 15408

27 ISO/IEC-versions of the CC standards

ISO/IEC 18045

28 ISO/IEC-version of the Common Evaluation Methodology

ISO/IEC 17065

29 For a Certification Body, ISO/IEC 17065 *Conformity assessment — Requirements for bodies certifying products, processes and services* applies according to the regulations of the EUCC scheme, and the Swedish Board for Accreditation and Conformity Assessment (Swedac), to ensure the quality of certifications.

ISO/IEC 17025

30 For an ITSEF, ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* applies according to the regulations of the EUCC scheme and Swedac, to ensure the quality of evaluations.

2.4.5 National Regulations - STAFS

31 The Swedish Board for Accreditation and Conformity Assessment (Swedac) has issued regulations for accreditation in the field of IT Security. These regulations are complements to the general regulations for accreditation.

Swedac STAFS 2020:1

Regulations and guidelines for accreditation.

2.5 Trademarks

32 Conditions for the use of trademarks applicable to the certification and licensing processes are listed in EP-070 *Conditions for Use of Trademarks*.

2.6 Documentation

33 This document provides an overview of the CSEC EUCC. Other documents described below give detailed information about other processes of the CSEC EUCC. All public External publications are available at the CSEC website, www.csec.se.

EP-301 Certification and Evaluation - EUCC - Overview

34 This document contains a general description of certification and evaluation under EUCC. It is the public top document of the CSEC EUCC certification regulations.

35 The document contains a brief description about the operations of the Certification Body and describes roles, definitions, and abbreviations important for the understanding of the information.

36 This is an informative document and is not to be regarded as controlling. It does not contain any information or specifications that are not declared or defined elsewhere.

EP-002 Evaluation and Certification

37 This document describes the policy and procedures for evaluations and certifications performed by the Certification Body. It provides sufficient information to each party in the evaluation and certification process; defining their responsibilities for maintaining a consistent and high quality and for cost effectiveness.

EP-003 Assurance Continuity

38 This document references the requirements and procedures for the continuous maintenance of certifications. This includes certificate maintenance, re-evaluation and re-assessment.

EP-004 Licensing of Evaluation Facilities

39 This document describes the requirements and procedures for licensing and for the maintenance of licenses of evaluation facilities.

EP-007 Quality Manual

40 This document describes the standard operating procedures of the Certification Body, satisfying the requirement from ISO/IEC 17065, that the Certification Body must have a Quality Manual.

41 This set of documents may be supplemented by documents addressing specific topics. For example, if evaluation of products at evaluation assurance levels (EAL) above EAL 4 is sought, or if evaluation of systems rather than products will be carried out, additional documents may be necessary. The goal of supplemental documents is to guide sponsors, developers, evaluators, and certifiers, so that requirements for the impartiality, objectivity, repeatability, reproducibility, and appropriateness of such evaluations can be guaranteed.

3 Types of Certifications

3.1 ICT Product Certification

42 The target of evaluation (TOE) consists of an entire ICT product or parts of an ICT product selected for CC evaluation, along with its associated administrator and user guidance documentation. An ICT product is a package of software, firmware, and/or hardware providing certain functionality.

43 The target of evaluation is defined in the context of a specific configuration or set of configurations, which is called the evaluated configuration of the target of evaluation.

44 The target of evaluation is evaluated in accordance with requirements contained in the CC. A security target (ST), a set of security requirements and specifications, is used as the basis for evaluating the target of evaluation. Investing substantial effort in creating the security target reduces the risk of running into problems later in the evaluation process. The goal of evaluation of a TOE is to demonstrate that the target of evaluation meets the security requirements contained in the evaluated security target. Successful evaluation following the rules of CSEC EUCC may result in certification of the product.

3.2 Protection Profile Certification

45 A protection profile is an implementation-independent set of security requirements for a category of ICT products that meet specific customer needs.

46 A protection profile may be created by

47 *"... the different stakeholders of ICT products cybersecurity certification may define Protection Profiles as technical specifications. Such technical specifications may be adopted as standards by a national, EU or International standardization organization (Reg. UE 1025/20124) and certified according to the requirements of this scheme. ENISA shall provide on its cybersecurity certification website a list of these Protection Profiles."* [ENISA] v1.1.1, chapter 3.

48 Sponsors then may claim compliance to the protection profile in their security targets (ST).

49 A protection profile is evaluated in accordance with the requirements for protection profile evaluation contained in the CC. The goal of such an evaluation is to demonstrate that the protection profile is complete, consistent, technically sound, and suitable for use as a statement of requirements for a category of ICT products. A successful evaluation following the rules of CSEC EUCC may result in certification of the protection profile.

4 Roles within CSEC EUCC

50 The parties involved in certifications under the CSEC EUCC fall into four categories: Sponsors, Developers, ITSEFs, and the Certification Body, each with its own specific role and responsibilities.

4.1 Sponsor

51 The Sponsor is the organisation that pays for the evaluation, applies to the Certification Body for certification, contracts with the ITSEF, and arranges for Developer participation. The Sponsor and the Developer may be the same.

52 The obligations of the Sponsor in an evaluation are detailed in External publication EP-002 *Evaluation and Certification*, section 3, Parties and Responsibilities.

4.2 Developer

53 The Developer is the organisation that produces the ICT product to be certified. The Developer, which may be the same as the Sponsor, is responsible for supporting the evaluation by making evaluation evidence available.

54 The obligations of the Developer in an evaluation are detailed in External publication EP-002 *Evaluation and Certification*, section 3, Parties and Responsibilities.

4.3 IT Security Evaluation Facility (ITSEF)

55 An Evaluation Facility licensed by the Certification Body to operate under the CSEC EUCC is called an ITSEF. The ITSEF is responsible for the assessment of the protection profile or the target of evaluation by performing the evaluator actions required by the CEM and the CSEC EUCC.

56 Further details of the obligations for ITSEFs and evaluators are found in External publication EP-004 *Licensing of Evaluation Facilities*, section 3, Parties and Responsibilities.

4.4 Certification Body

57 The Certification Body provides independent confirmation of the validity of evaluation results by overseeing the evaluation process. This oversight is performed by certifiers working for the Certification Body.

58 A more extensive presentation of the responsibilities of the Certification Body is found in the following External publications.

- EP-002 *Evaluation and Certification*
- EP-003 *Assurance Continuity*
- EP-004 *Licensing of Evaluation Facilities*
- EP-007 *Quality Manual*

5 Processes within the CSEC EUCC

5.1 Management of Confidential Information

5.1.1 Legal Protection of Confidential Information

59 Documents received or drawn up by the Certification Body are official documents ("*allmän handling*") and may be kept secret by the Certification Body only when it is required to protect the interests covered by articles in The Swedish Law on Publicity and Secrecy regarding the following.

- The security of the realm or its relationships with another state or international organisation
- Inspection, control, or other supervisory activities of a public authority
- The prevention or prosecution of crime
- The economic interests of the public institutions
- The protection of the personal or economic circumstances of private subjects

60 When a request is made by a third party for access to an official document, the Certification Body judges whether the information is confidential given the conditions at that time.

61 Information deemed confidential according to the act SHALL be kept secret, while information not covered SHALL be disclosed to the requesting party in accordance with *The Freedom of Press act*.

62 Before exchanging confidential information with the Certification Body, the information owner MAY seek advice from the Certification Body on the applicability of Swedish Law on the information.

63 If the identity of a party (sponsor, developer etc) is to be treated as confidential this SHALL be noted to the Certification Body prior to any correspondence commencing.

64 The confidentiality requirements between the ITSEF, Sponsors, and Developers SHOULD be defined in detail in agreements between the parties.

65 More information on legal protection of confidential information is described in EP-007 *Quality Manual*.

5.1.2 Protective Marking of Confidential Information

66 Originators of information SHALL make the Certification Body aware of any confidentiality claims regarding information that is shared with the Certification Body as follows.

- Documents with confidentiality claims regarding the entire document or parts thereof SHALL bear protective marks indicating that the information should be regarded as confidential.
- The originator is to clarify their claims on confidentiality to the Certification Body by presenting a justification describing the parts of the document covered by the security claims. A brief statement outlining the nature of the damage which would result from disclosure can be added.
- The applicable articles in The Swedish Law on Publicity and Secrecy MAY be added to the statement to help the Certification Body in forming its judgement when applying a security classification.

67 If the identity of a party (sponsor, developer etc) is to be treated as confidential this SHALL be clarified with the Certification Body before any correspondence commences.

5.1.3 Sending Confidential Information by Mail

68 Documents containing confidential information sent via standard post ("A-post") SHOULD be sent using two enclosed envelopes as follows.

- The outer envelope SHOULD carry the address of the Certification Body and MAY have the name of the addressee (Certification Body Point-of-Contact) on top of the address.
- The inner envelope SHOULD bear a protective mark indicating that the information should be regarded as confidential, carry the address of the Certification Body and have the name of the addressee on top of the address as follows.

<Name of the addressee>
Swedish Certification Body for IT Security
FMV/CSEC
SE-115 88 Stockholm, Sweden

5.1.4 Electronic Transmission of Confidential Information

69 Any use of electronic transmission of confidential information SHALL be agreed with the Certification Body before any correspondence commences.

5.2 Certification Agreement

70 According to the rules and regulations for accreditation the Certification Body SHALL have a legally enforceable Agreement for the provision of certification activities with its clients.

71 This Agreement is established as follows.

1. The Sponsor signs and submits an Application for Certification to the Certification Body, and thereby accepts compliance with the clients' responsibilities, as defined in EP-002 *Evaluation and Certification.*
2. The Certification Body decides, depending on complexity of the ICT product to be certified and the AVA_VAN, the fees for the certification and sends a Tender to the Sponsor.
3. The Sponsor sends an acceptance of the fee and the terms of the Tender, in writing, to the Certification Body.

72 These three documents together form the Certification Agreement.

5.3 Evaluation and Certification Process

73 The IT security evaluation is the process of assessing a protection profile or target of evaluation against defined criteria.

74 The criteria used for evaluations are those of the CC and the CEM, supplemented by additional requirements and specialisations in the CSEC EUCC procedures for evaluation and certification.

75 Every completed certification will result in a certification report; for successful certifications, a certificate will be issued for the ICT product or protection profile.

76 The evaluation and certification process consists of three phases as follows.

1. Start-of-evaluation The four parties involved in the evaluation and certi-

	fication (Developer, Sponsor, ITSEF, and Certification Body) prepare for evaluation.
2. Conduct of evaluation	The evaluation is performed.
3. Conclusion of evaluation	The evaluation is completed.

77 Evaluations may be carried out on a target of evaluation that has already been finished, or in parallel with target of evaluation development (i.e., concurrent evaluation).

78 The detailed evaluation and certification process is described in External publication EP-002 *Evaluation and Certification*.

5.3.1 Cost of Evaluation and Certification

79 The total cost of evaluation and certification includes the following.

- The Developer's and Sponsor's internal costs for the preparation and conduct of the evaluation, including document updates, bug fixes, additional testing, etc.
- The evaluation cost, covering the ITSEF's work
- The certification cost, covering the Certification Body's work

80 The internal costs to the Sponsor and the Developer may be substantial and should be taken into account; however, discussion of those costs is outside the scope of this document. The cost for the ITSEF's work will be agreed between the Sponsor and the ITSEF, but should be free from undue conditions that may impact the ITSEF's impartiality.

81 The Certification Body's charges and fees for certification, including Application Fee and Certification Fee, are described in External publication EP-008 *Charges and Fees*.

5.3.2 Official Languages of the CSEC EUCC

82 Evaluation reports, oversight reports, and certification reports may be written in Swedish or English.

83 Other languages may be used in evaluation evidence and other documentation related to the certification, but must be made available in either Swedish or English if required by the Certification Body.

5.4 Certificate Validity

84 The maximum period of validity of EUCC certificates is five years.

85 A shorter maximum period of validity may be specified within a specific Technical Domain.

5.4.1 Valid certificates

86 Valid certificates will be disclosed, together with the related certification report and any relevant information by:

- ENISA in a dedicated website on European cybersecurity certification schemes (according to [ENISA] v1.1.1, chapter 20)
- CSEC EUCC on the Certified Products List (CPL) on the CSEC EUCC website
- NCCA on <TBD>

5.4.2 Expired certificates

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

- ENISA in a different webpage than the valid ones on European cybersecurity certification schemes (according to [ENISA] v1.1.1, chapter 20)
- CSEC EUCC in the list of Archived certificates on the CSEC EUCC website

- NCCA on <TBD>

5.4.3 Extended period of validity

88 The process of Assurance continuity, which are detailed in section 5.6, allows for extending the administrative validity of a certificate.

5.5 Compliance monitoring

89 The Certification Body will perform compliance monitoring. This compliance monitoring should cover the following:

- *"a non-compliance in the application by a manufacturer or provider of the rules and obligations related to a certificate issued on their ICT product;*
- *a non-compliance in the conditions under which the certification takes place and that are not related to the individual ICT product;*
- *a non-conformity of a certified ICT product with its security requirements, which includes and is not limited to a:*
  - *change in the threat environment after the issuance of the certificate, which has an adverse impact on the security of the certified ICT product;*
  - *vulnerability identified and related to the certified ICT product, that has an adverse impact on the security of the certified ICT product."* [ENISA] v1.1.1, chapter 11

5.6 Assurance continuity

90 *"Assurance continuity seeks to exploit the fact that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. The assurance continuity paradigm therefore defines the processes for certificate maintenance through re-evaluation and re-assessment such that each seeks to recognise previous evaluation work."* [ENISA] Annex 11, 2.3

5.6.1 Certificate maintenance

91 *"Certificate maintenance activities refer to the process undertaken by a developer in order to have a TOE, listed in the maintenance addendum for that TOE. It must be demonstrated that the changes to the TOE, the IT environment and/or the development environment do not adversely affect the assurance baseline."* [ENISA] Annex 11, 2.3

92 If a certified product or its intended environment is changed, without affecting the assurance in the product, the validity of the certificate may be extended to incorporate the changed version of the product. To do this, a maintenance impact analysis report and a maintenance application have to be submitted to the Certification Body. If the Certification Body accepts extension of the certificate validity, a maintenance addendum, including a maintenance report, will be published in the certified products list on the CSEC website. If the certificate cannot be extended, a re-evaluation re-using previous evaluation results or a new full certification may be performed. The procedures for certificate maintenance are described in detail in EP-002 *Evaluation and Certification*

5.6.2 Re-evaluation

93 *"Re-evaluation refers to the evaluation of a changed TOE, such that the developer could not (or chooses not to) demonstrate that changes to the certified TOE do not adversely affect the assurance baseline."* [ENISA] Annex 11, 2.3

94 A *re-evaluation* may be conducted when another version of an already-certified product shall be evaluated. This may be the case for a new version of an ICT product with modified functionality, a revised intended environment, or for additional platforms.

5.6.3 Re-assessment

95 *"Re-assessment refers to the evaluation of a previously certified TOE against a changed threat environment."* [ENISA] Annex 11, 2.3

5.7 Licensing of Evaluation Facilities

96 Licensing of evaluation facilities is the formal process whereby the Certification Body grants an Evaluation Facility the right to conduct CC evaluations under the CSEC EUCC, thus becoming a licensed ITSEF. Before the Certification Body issues a license, the ITSEF must be accredited by a recognised accreditation body as a test laboratory according to ISO/IEC 17025. This whole process guarantees that the evaluators of an ITSEF will carry out impartial, objective, repeatable, and reproducible evaluations. Developers and Sponsors will then be able to trust the ITSEF to provide professional work and effective results.

97 Within the scope of CSEC EUCC, an ITSEF may conduct evaluations at:

- AVA_VAN.3
- AVA_VAN.4 and AVA_VAN.5 based on a Protection Profile laid down in Annex 16 of [ENISA]

98 The technical domains *smart cards and similar devices* and *hardware devices with security box* are not covered by CSEC EUCC.

99 The CSEC EUCC leaves differentiation of ITSEF skills to market forces and assumes that Sponsors will select appropriate ITSEFs to perform evaluations. A list of ITSEFs will be available from the Certification Body.

100 Prior to each evaluation, the ITSEF must demonstrate to the Certification Body that the resources assigned to the project have appropriate skills and background to complete the evaluation.

101 Thus, before the evaluation starts, the Certification Body will assess the combined skills of the evaluation team in relation to the evaluation and may require that the staffing is justified by the ITSEF.

102 The details of the ITSEF licensing process are described in External publication EP-004 *Licensing of Evaluation Facilities*.

5.8 Scheme Notes

103 A Scheme Note is a non-trivial clarification of the contents of the CC, the CEM, or the operation of CSEC EUCC. Scheme Notes must be documented and taken into consideration when a similar clarification is made, to ensure consistency over time in the application of the evaluation criteria.

104 All Scheme Notes will be presented to the Change Control Board for comments, before they are published.

105 Scheme Note issues will normally be raised by the Certification Body staff and have their origin in on-going evaluations, but all relevant issues brought to the attention of the Certification Body will be considered.

5.9 Complaints and Appeals

106 The purpose of the procedures for management of complaints and appeals is to ensure that:

- the Certification Body has suitable policies and procedures for the resolution of complaints and appeals,
- details of the procedures for handling complaints and appeals are documented and published according to applicable standards,
- the Certification Body has procedures to correct decisions that are not made according to the rules of the CSEC EUCC, and
- the Certification Body has procedures to learn from any complaints or appeals and to update the CSEC EUCC accordingly.

Complaints

107 The Certification Body will document and investigate any complaint directed towards it that applies to the certification activities for which it is responsible.

108 The Certification Body is responsible for investigating all such complaints in order to identify possible nonconformities to CSEC EUCC regulations. Any nonconformity found will be subject to the procedures for handling of nonconformities.

109 The procedures for handling Complaints are described in EP-007 *Quality Manual*.

Appeals

110 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 Body is responsible, may file an appeal.

111 An appeal shall be made in writing and shall contain the name, address, and telephone number of the appellant. It shall identify and describe the requested changes to the decision that is being appealed.

112 Contact information for the Certification Body and forms for complaints and appeals will be found on the CSEC web site, www.csec.se. Use of these forms is recommended, but not mandatory.

113 The procedures for handling Appeals are described in EP-007 *Quality Manual*.

Appendix A

A.1 References

These references are common to all public CSEC EUCC documents.

Reference	Description
CC	Common Criteria for Information Technology Security Evaluation
CC Part 1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model
CC Part 2	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements
CC Part 3	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements
CEM	Common Methodology for Information Technology Security Evaluation
CSA	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
ISO/IEC 17065	Conformity assessment — Requirements for bodies certifying products, processes and services. The most recent version is ISO/IEC 17065:2012.
EP-301	Certification and Evaluation - EUCC - Overview
EP-002	Evaluation and Certification
EP-003	Assurance Continuity
EP-004	Licensing of Evaluation Facilities
EP-007	Quality Manual
EP-008	Charges and Fees
EP-070	Conditions for the Use of Trademarks
ENISA	CYBERSECURITY CERTIFICATION EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS
IA	COMMISSION IMPLEMENTING REGULATION (EU) …/... of XXX establishing the Common Criteria-based European cybersecurity certification scheme (EUCC)
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories. The most recent version is ISO/IEC 17025:2018
STAFS 2020:1	Styrelsen för ackreditering och teknisk kontrolls föreskrifter och allmänna råd om ackreditering

A.2 Abbreviation

The following abbreviations are used in this document and other CSEC documents.

Abbreviation	Term or concept
AVA_VAN	Assurance Family "Vulnerability Analysis"
CERT	Computer Emergency Response Team
CB	Certification Body
CC	Criteria (CC Part 1-3 refers to the Common Criteria standard documentation)
CAB	Conformity Assessment Body
CEM	Common Methodology for Information Technology Security Evaluation
CSA	CyberSecurity Act
CSEC	Swedish Certification Body for IT Security
CSEC EUCC	CSEC Common Criteria based European cybersecurity certification
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
CV	Curriculum Vitae
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
EP	External Publication
ETR	Evaluation Technical Report
EUCC	Common Criteria based European cybersecurity certification
EUCC scheme	Common Criteria based European candidate cybersecurity certification scheme
EWP	Evaluation Work Plan
FER	Final Evaluation Report
FMV	Försvarets Materielverk - The Swedish Defence Materiel Administration
IAR	Impact Analysis Report
ICC	
ICT	Information and communications technology
IT	Information Technology
ITSEF	Testing Laboratory / Evaluation Facility
NCCA	National Cybersecurity Certification Authority
PP	Protection Profile
SAC	Scheme Advisory Committee
SAR	Security Assurance Requirement
SER	Single Evaluation Report
SFR	Security Functional Requirement
SN	Scheme note
ST	Security Target
Swedac	Swedish Board for Accreditation and Conformity Assessment
TOE	Target of Evaluation
TOR	Technical Oversight Report
TSF	TOE Security Functions
TSFI	TOE Security Functional Interface

Abbreviation	Term or concept
TSP	TOE Security Policy

A.3 Glossary

Glossary	
Concurrent evaluation	An evaluation of a target of evaluation (TOE) that is in development.
Cross frontier evaluation	An evaluation where work is performed in locations situated outside Sweden.
EUCC certificate	a European cybersecurity certificate issued under the EUCC scheme
Initial evaluation	An evaluation of a target of evaluation or a protection profile (PP) that has not previously been evaluated.
Protection profile	An implementation-independent set of security requirements for a category of targets of evaluation that meet specific consumer needs. [CC]
Re-evaluation	An evaluation of a new version of an already evaluated target of evaluation.
Security target	A set of security requirements and specifications to be used as the basis for evaluation of an identified target of evaluation. [CC]
Target of evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC]