CCC SP-101-3

Singapore Common Criteria Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

Publication No. 3

Evaluation and Certification

June 2024
Version 8.0

Amendment Record

Version	Date	Author	Changes
1-3	August, 2009	Infocomm Development Authority of Singapore	Release
4.0	October, 2017	Cyber Security Agency of Singapore	Alignment to CSA processes.
5.0	June, 2018	Cyber Security Agency of Singapore	Revision to Annex H, Impact Analysis Report. Minor editorial amendments
6.0	January 2019	Cyber Security Agency of Singapore	Revision to the use of protective marks, logos and advertisement
7.0	December 2019	Cyber Security Agency of Singapore	Minor editorial revisions
7.1	May 2024	Cyber Security Agency of Singapore	Minor editorial revisions
8.0	June 2024	Cyber Security Agency of Singapore	Transition to CC:2022

Contents

1 INTRODUCTION

1.0.1 The certification of IT products shall be performed within the framework of the Singapore Common Criteria Scheme (SCCS). The SCCS is owned and managed by the Evaluation Authority under the ambit of Cyber Security Agency of Singapore (CSA). CSA also provides the services of an Evaluation Authority which independently validates the evaluation results produced by the approved Common Criteria Testing Laboratory (CCTL) and the issuance of certificates.

1.0.2 The key roles and responsibilities for the certification procedure are:

a. Evaluation Authority: The Evaluation Authority is the Scheme owner and oversees the entire operations of the scheme. The Evaluation Authority accepts applications for certification into SCCS, provides oversight on the procedures, supervises the evaluation work of the CCTL, and issues the final certificate. For every evaluation, responsible and fully qualified certifiers are assigned to ensure that the evaluation by the CCTL adheres to SCCS standards and requirements. The certifiers may advise the CCTL on any process or technical issues. However, they will not perform the evaluation itself. The tasks to be done and the degree of involvement in certification will vary from one evaluation project to another. Optional verification and validation activities could be done at the discretion of the certifiers. The main responsibilities of the certifiers are to supervise and to qualify the evaluation activities of the evaluation team, to provide methodical guidance to the evaluation team on evaluation issues and in such a way to ensure that the evaluation by the CCTL adheres to SCCS standards and requirements. The certifiers produce a Certification Report (CR) at the completion of the evaluation process.

b. Common Criteria Testing Laboratory (CCTL): The CCTL is an independent commercial test laboratory which is approved under the SCCS. The CCTL evaluates the deliverables provided by a sponsor/developer according to the CC standards and reports its results to the Evaluation Authority and the developer. The results can only be: pass, fail, and inconclusive. ‘Fail’ and ‘inconclusive’ requires corrective actions on the side of the developer; the CCTL must clearly inform the developer on the cause of or reason for the verdict, but must not provide recommendations or solutions.

c. Sponsor: The sponsor is the entity which officially requests for the certification and evaluation of the product and enters into separated contractual relationships with the Evaluation Authority and CCTL. The sponsor is responsible for timely submission of deliverables, updates on the project status and for the payment of relevant fees (e.g. certification fees, evaluation fees). The sponsor may be the risk owner of an IT system, the developer of the product or an agency of

the Singapore Government which funds the certification and evaluation.

d. Developer: The developer is the entity which develops, manufactures or creates the Target of Evaluation (TOE), together with the deliverables required by the SCCS for evaluation and supports the CCTL for the conduct of the evaluation (e.g. specifications, test scripts, samples of TOE etc.). The developer may, but need not be, the sponsor.

e. Consultant: A developer/sponsor may engage a consultant to work on or provide guidance regarding the deliverables required by the CCTL or the Evaluation Authority. The consultant may be nominated as the contact person of the developer/sponsor, in which case the consultant shall be deemed fully empowered by the sponsor to represent the interests of the developer and sponsor. The Evaluation Authority may communicate with, and rely on the understanding and decision of the consultant as if the consultant is the developer and sponsor, without further reference to either the developer or sponsor.

f. Evaluation Working Group: Each of the sponsor, developer (if the sponsor is not the developer), CCTL, and Evaluation Authority shall nominate one (1) person to represent the respective stakeholders.

2 SCOPE

2.0.1 This document sets out the security requirements and procedures for the evaluation and certification of IT products under the SCCS, namely, the pre-evaluation/evaluation application phase, evaluation phase, conclusion phase, award of certificates, assurance continuity maintenance and re-evaluation. It also establishes the technical oversight role of the Evaluation Authority in the SCCS and sets out general terms and conditions that apply to the sponsor and/or CCTL that participate in a certification project or an Assurance Continuity project.

3 IT SECURITY EVALUATION AND CERTIFICATION

3.1 Pre-Evaluation Phase

3.1.1 Feasibility Study

a. If a sponsor wishes to obtain certification of an IT product under the SCCS, it must engage a CCTL to perform the evaluation tasks required for certification. The terms of engagement shall be as negotiated between the sponsor and the CCTL. CSA Evaluation Authority will not be involved in any contractual arrangements between the sponsor and the CCTL nor shall CSA Evaluation Authority be a party to the contract between the sponsor and the CCTL.

b. To be evaluated under the SCCS, products should preferably:

   i. Claim conformance to a National Protection Profile approved by CSA; or

   ii. Claim conformance to an endorsed collaborative Protection Profile (cPP); or

   iii. Claim conformance to a certified Protection Profile [1] (PP) recognised / approved by CSA.

c. Products not claiming conformance to any of the above (i.e. Security Target (ST) only evaluations) may be accepted, with assurance claims up to Evaluation Assurance Level 2.

d. Product not claiming conformance to any of the above (i.e. ST only evaluations) with assurance claims higher than Evaluation Assurance Level 2 may only be accepted on a case-by-case basis (e.g. explicit written requirement by a Singapore Government Agency).

e. Developer shall implement flaw remediation procedures (i.e. augmentation with ALC_FLR).

f. Developer shall confirm that all known vulnerabilities have been fixed for the TOE or that vulnerabilities do not affect the TOE.

g. If the TOE is implemented with universal default password, the TOE shall mandate users to change password during the TOE provisioning phase.

[1] The Protection Profile has to be certified by a CC scheme or developed by other relevant Singapore Government agencies.

h. The TOE shall be implemented with best practice cryptography algorithm(s), network protocol(s) and standard key length.

i. The TOE shall be using up-to-date third-party components as far as possible. Developer shall provide justification for any third-party components that are not up-to-date, where applicable.

j. The PP, ST and TOE are described in more details in SCCS Publication #1 and in CC Part 1. The evaluation of a TOE may be carried out after the TOE development has been completed or in parallel with the TOE development.

k. The sponsor is required to provide the CCTL with (a draft of) the ST, applicable evaluation deliverables and any other evidence that the TOE has been designed and implemented to meet the requirements of the CC and cPP (if applicable). Depending on the Evaluation Assurance Level (EAL) and the necessary assurance activities to be performed, the sponsor may be required to provide the following to the CCTL:

    i. Access to hardware, software and firmware necessary for the CCTL to undertake independent functional and penetration testing of the TOE;

    ii. Development documentation describing configuration control, programming languages, compilers and developer security;

    iii. Administration and user documents required for installing, configuring and using the TOE;

    iv. Supporting and technical documents generated during the development of IT product;

    v. Operational documents needed for delivery, configuration, start-up and operation;

    vi. Evidences of security engineering, including justifications, conformance analysis report, proofs and testing materials.

l. The CCTL may conduct a feasibility study based on the evidence provided by the sponsor to determine the scope and cost of evaluation. Based on the supplied evidences, the CCTL assesses the suitability and completeness to determine whether the evaluation could be conducted in accordance to the CEM and within the proposed time frame.

3.1.2 Application for Certification

a. Application or enquiry for IT security certification under the SCCS should be addressed to the Evaluation Authority at the following

address:

The Technical Manager,
Singapore Common Criteria Scheme
Cybersecurity Certification Centre
Cyber Security Agency of Singapore (CSA)
5 Maxwell Road MND Complex #03-00 Tower Block
Singapore 069110

or

sccs@csa.gov.sg

b. The sponsor for an IT product shall submit to the Evaluation Authority the application package, which at least consists of:

i. The Certification Application Form (CAF), duly signed by the CCTL, the Sponsor, and the developer (where the sponsor is not the developer)

ii. An ST prepared in accordance with the requirements set out in the CC Part 1;

iii. A provisional Evaluation Work Plan (EWP), outlining the evaluation tasks to be performed according to the CC CEM and a timeline. As a general rule, an evaluation project at EAL 2 or equivalent (based on the assurance activities defined in the cPP) should not take longer than 6 months to complete;

iv. A preliminary assessment by the CCTL on the ST and the sufficiency of the evidences provided. The assessment shall cover the key criteria for ASE to a suitable level of detail and shall provide information about potential or actual concerns about the project, staff, TOE and/or the sufficiency of the evidences. The assessment shall also highlight the CCTL's assessment on the applicability of any Supporting Documents[2];

v. For software TOE, the binary shall be provided to the Evaluation Authority;

vi. The Impact Analysis Report, if the application is meant for Assurance Continuity.

3.1.3 Review of the Application for new certification[3]

[2] 'Supporting Documents' are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.

[3] Application for Assurance Continuity is described in Chapter **Error! Reference source not found.**.

a. Upon receiving the completed application package, the Evaluation Authority will review and determine that:

   i. The application form is duly completed and signed by all parties (i.e. Sponsor, Developer and CCTL);

   ii. The ST comprises all major content items defined in the CC Part 1;

   iii. The TOE has been clearly identified in the ST; threats and security requirements are defined in the ST in terms of assets, threat agents, attack potential and countermeasures;

   iv. Conformance claims in the ST are made accurately;

   v. Evaluation activities can be adequately set up for the TOE to be performed by the CCTL to the specified evaluation assurance level/activities;

   vi. The CCTL has given a positive statement on the suitability and completeness of the TOE documentation such that detailed evaluation can be performed and completed within the timeframe stated in the EWP; and

   vii. The evaluation can yield objective and unbiased evaluation results.

   viii. The evaluators appointed by the CCTL for the evaluation are qualified/approved under the SCCS. The related information on each evaluator assigned by the CCTL for the evaluation procedure in question shall be provided by the CCTL to the Evaluation Authority.

b. The EWP may evolve during the evaluation process. It is the sponsor and/or developer's responsibility to ensure that the CCTL always has the latest information about the TOE. The CCTL is expected to interact with the Evaluation Authority, as and when issues arise and clarifications need to be made. Any amendments to the TOE that have an impact on EWP during evaluation must be highlighted to the Evaluation Authority. Approvals by the Evaluation Authority shall be sought for any changes to the EWP which have an impact on evaluation work.

c. The sponsor may engage a consultant to provide advice and consultation services in developing the ST and other evaluation deliverables; The CCTL is allowed to provide both consultancy and evaluation services for the same TOE under the SCCS if the CCTL is able to demonstrate its conformance to 2.2.1 and 2.4 of the SCCS Publication #2 with clear role and logical separation procedures in place as well as appointing qualified evaluators and qualified

consultants for the project.

d. If the Evaluation Authority decides to accept the evaluation under the SCCS, a unique identifier will be assigned. In addition, the Evaluation Authority will issue a “Letter of Acceptance” to the sponsor and a confirmation to the CCTL. The Evaluation Authority shall assign one or more of its staff members to act as certifier(s), whose role is to oversee the evaluation. If otherwise, the application for evaluation is not deemed accepted by the SCCS and no further action need to be taken by the Evaluation Authority with respect to the evaluation under the SCCS.

e. Full payment of the requisite certification fees shall be received by CSA prior to the Task Kick-off Meeting. The fee payable to the Evaluation Authority does not include any fees or charges which the sponsor has to pay to the CCTL or any third-party consultant. The fee covers the reasonable costs and expense of the Evaluation Authority’s travel and meeting arrangement within Singapore. Additional fees may apply if the certifier is expected to travel overseas.

3.1.4 Task Kick-off Meeting

a. After accepting the TOE for evaluation and certification under the SCCS, the Evaluation Authority will contact members of the evaluation working group (namely the sponsor/developer and the CCTL) for the evaluation Task Kick-off Meeting (TKM). The outline for a typical TKM agenda is given in Annex A.

b. The TKM enables all the parties concerned to come together to discuss and confirm the EWP and gain a common understanding of the evaluation scope. The sponsor is responsible for providing all the evaluation deliverables listed in the EWP to both the CCTL and the Evaluation Authority. Based on the EWP, the Evaluation Authority will inform the CCTL of the evaluation tasks which the Evaluation Authority plans to observe, the planned evaluation progress meetings and any scheduled visits to the CCTL facilities for performing independent testing and evaluation work. The CCTL shall provide the secretariat function to record the minutes and circulate it for confirmation by members of the meeting.

c. The parties shall, during the TKM, address the applicability of Supporting Documents to the project and whether any third party would need to be involved in the project, for example, where the third party’s specialised equipment or knowledge is needed for the project. The main objective is to establish, among all parties, a sufficiently clear and common understanding of all additional factors for the project.

d. As part of the Evaluation Authority’s role to perform oversight on the

evaluation work and ensure comparability among the evaluation work performed by the CCTLs, the Evaluation Authority may need to attend on-site evaluation activities conducted by the CCTL, whether in Singapore or overseas. The parties shall, during the TKM, also address the need of overseas travel by the Evaluation Authority.

3.2 Evaluation Phase

3.2.1 Evaluation Tasks

a. The evaluation phase begins only upon the closure of a successfully conducted TKM and subject to all applicable certification fees having been paid in full. A TKM is regarded as successfully conducted when the TKM minutes have been approved by the Evaluation Authority, the sponsor, and the CCTL, and the Evaluation Authority is satisfied that all open issues arising from the TKM have been sufficiently addressed. Thereafter the Evaluation Authority will update the Evaluation Product List (EPL) and list the product as 'under evaluation', and the CCTL shall perform the evaluation tasks indicated in accordance with the EWP (with milestones indicated) as approved by the Evaluation Authority, and in accordance with the CC and the CEM.

b. Evaluation Progress Meetings (EPM) may be initiated by any of the parties involved, and shall be attended by all members of the evaluation working group. A typical EPM agenda outline is given in Annex B. EPMs will be scheduled and chaired by the Evaluation Authority. The CCTL shall provide the secretariat function to record the minutes and circulate it for confirmation by members of the meeting.

c. At least one (1) EPM is expected to be held after completion of the ASE, one (1) EPM before ATE (Assurance Class Test) & AVA (Assurance Class Vulnerability assessment) commence, and one (1) EPM after ATE and AVA are completed. The CCTL shall provide the test plan for ATE and AVA at least 2 weeks (or if requested by the Evaluation Authority, earlier) before the EPM to the Evaluation Authority.

d. Additional EPMs may be held as and when the need arises.

e. The outcome of each evaluation task is recorded in a Single Evaluation Report (SER). The outline for the SER is given in Annex C. Alternative reporting procedures are supported as long as the requirements in Annex G are fulfilled.

f. There will be instances whereby the CCTL will conduct a site visit to the developer's premises and any other contributing development or manufacturing sites. The Evaluation Authority reserves the right to attend such site visits. The cost of travel, accommodation and

expenses for the Evaluation Authority staff attending a site visit outside of Singapore will be borne by the sponsor. The Evaluation Authority may call an EPM before a site visit is conducted and the CCTL shall submit the site visit plan to the Evaluation Authority at least 2 weeks before the EPM or the actual site visit (whichever is earlier).

g. If the sponsor is not the developer of the IT product, the sponsor shall be solely responsible for ensuring that all evaluation deliverables and access to information from the developer are provided to the CCTL and the Evaluation Authority.

h. The CCTL shall manage the evaluation work and deliverables in accordance with ISO/IEC 17025.

3.2.2 Single Evaluation Report

a. At the end of each evaluation task, the Single Evaluation Report (SER) as outlined in Annex C shall be submitted by the CCTL to the Evaluation Authority. The CCTL shall use the SER to report on the verdicts of all the evaluation activities performed for a particular evaluation task according to the EWP, the CC and CEM. The CCTL shall provide justification for all verdict (either as part of the SER, or in the case of a verdict of 'fail' or 'inconclusive' as a separate Observation Report (OR) containing the information set out in Annex D).

b. The Evaluation Authority will review the SER (and the OR if applicable) and may request for more evaluation evidence from the CCTL or the sponsor if necessary. The outcome of the review will be recorded in a SER Review Report (RR) shown in Annex F, and a copy of such report will be given to the CCTL. If the SER (and the OR, if applicable) contains incomplete or incorrect information, the Evaluation Authority will require a revised version to be submitted by the CCTL.

c. For any independent testing (functional or penetration testing) required to be performed on the TOE, the CCTL shall include the following in the SER for that particular evaluation task. It shall contain the necessary and sufficient to ensure that the tests are repeatable and reproducible (by another personnel external of the CCTL) and results are consistent.

    i. A test plan describing the activities involved in executing the tests with sufficient details for ensuring repeatability and reproducibility;

    ii. Testing requirements describing the test inputs which may include hardware, software, firmware, documents and environment;

iii. Testing methodology for implementing the test plan according to the CEM;

iv. Test tools and configuration used, involving hardware, software, firmware and environment where necessary. When applicable, the model number, serial number, version number, settings, etc. of the test tools (software and hardware) used should be recorded accordingly;

v. Test scripts describing the steps in which tests are carried out; and expected outputs for each test in comparison with the actual outputs obtained as a result of the test; and

vi. Location and set-up of the test execution.

d. Any exploitable vulnerability discovered shall be clearly reported in detail, including the efforts required for successful exploitation.

e. Any security vulnerability discovered shall be resolved by the developers. The CCTL shall provide justifications for any exceptions. The justifications are subjected to approval by the Evaluation Authority.

3.2.3 Evaluation Technical Report

a. Once the CCTL has completed all the evaluation tasks scheduled in the EWP, the CCTL shall generate an Evaluation Technical Report (ETR) containing the information set out in Annex E. The ETR shall include information derived from the SERs and ORs generated during the evaluation. The ETR shall be submitted to the Evaluation Authority. The ETR content shall conform to the requirements of the CEM.

b. The CCTL shall ensure that the vulnerability analysis (AVA_VAN) required under the CEM shall be performed and completed within 6 months prior to the date of submission of the ETR (or the revised ETR, if applicable). Otherwise, the CCTL shall conduct a fresh AVA_VAN.

c. The Evaluation Authority reviews the ETR and the outcome is recorded in an ETR Review Report (RR), and a copy will be given to the CCTL. The outline for the ETR RR is shown in Annex F. If the ETR contains incomplete or incorrect information, the Evaluation Authority will require a revised version of the ETR to be submitted by the CCTL.

d. For projects which require international recognition (or candidates for shadow assessments or Voluntary Periodic Assessment (VPA)), the CCTL must be accredited to ISO/IEC 17025, before it can submit the

final and official ETR to the Evaluation Authority.

3.3 Conclusion Phase

3.3.1 After the ETR has been approved by the Evaluation Authority, a Task Close-down Meeting, outline as shown in Annex H, will be arranged. During this EPM, the CCTL will provide a summary of all the evaluation tasks performed and highlight any problem encountered during the evaluation.

3.3.2 The ETR approved by the Evaluation Authority will be used by the Evaluation Authority as the basis for preparing the Certification Report (CR). The CR specifies the scope of evaluation and contains the final verdict of the evaluation indicating whether certification will be awarded or not. It may include recommendations for the secured use of the TOE constrained by the environment and the platform in which the TOE is to be used. The CCTL may be called upon to provide the necessary technical support to generate the CR.

3.3.3 The CR confirms that the evaluation has been conducted in accordance with the SCCS and that the conclusions drawn from the evaluation are consistent with the facts presented. The contents of the CR shall be in accordance with the CCRA requirements. Copyright in the CC Certificates and Certification Reports remains the property of CSA at all times.

3.4 ST Sanitisation

3.4.1 For international recognition of a TOE under the CCRA, a ST must be published along with the certificate. However, it is recognised under the SCCS (and also CC/CCRA) that in certain cases a ST may carry confidential or proprietary implementation details required for an evaluation.

3.4.2 To protect such sensitive and proprietary information, there exists an option to generate and publish a so-called ‘sanitised’ ST without such confidential or proprietary information. A sponsor who wishes to make use of this option must inform the Evaluation Authority and provide the sanitised ST to the Evaluation Authority *before* the CCTL submits its ETR to the Evaluation Authority. The CCTL shall assist in the assessment and approval process in relation to the sanitised version of the ST.

3.5 Information Sanitisation

3.5.1 It is further recognised under the SCCS that, where a sponsor is different from a developer, evaluation information and results from CCTL, ORs, ETR, etc., may also contain sensitive or proprietary information belonging to the developer. Such information may require sanitisation before it is given to a sponsor. It is for the sponsor, developer, and the CCTL to agree amongst themselves whether any such information requires sanitisation and to carry out any such sanitisation. However, where any

such sanitisation is carried out, both the original and the sanitised versions (with each version clearly marked as such) shall be provided to the Evaluation Authority.

3.6 Awarding of Certificate

3.6.1 Preparation

a. When the evaluation is completed, the process of awarding the CC certificate begins. The Evaluation Authority will prepare a file, comprising:

   i. Certification Application Form (CAF);

   ii. Final version of the Security Target;

   iii. Evaluation Technical Report;

   iv. Certification Report; and

   v. Prepared CC certificate

b. The file will be reviewed and validated by the Technical Manager of the Evaluation Authority, before submitting to the Head of the Evaluation Authority for approval and award of the CC certificate.

3.6.2 Certification Approval

a. The Head of the Evaluation Authority will decide whether or not to approve the certification, and if the approval is granted, will sign the Certification Report and the CC certificate[4].

3.6.3 Issuance and Publication of Certificate

a. The original CC certificate and the Certificate Report will be issued to the sponsor. The certificate will name the developer as the product developer in the certificate. Unless the sponsor has indicated in the CAF that the existence of the certification project is confidential, the Certified Product List (CPL) for SCCS available on CSA's website shall be updated and the Evaluation Authority will inform other Evaluation Authorities within the CCRA partnering countries of the publication of the CC Certificate.

3.6.4 Certificate Validity

a. Certificates are valid for a period of 5 years from the date of issue.

[4] Until SCCS is accepted as a CCRA authorising member, the certificate will not bear the CC/CCRA logos.

Validity could be extended by means of Assurance Continuity.

b. While the general validity is for a period of 5 years, certificate could be revoked if any of the conditions in Section 6.1.1 is met.

3.6.5 Changes to Conditions for Certification

a. The Evaluation Authority reserves the right to make changes to SCCS Publications and to any conditions for certification under the SCCS. If such changes substantially affect ongoing evaluation activities, the Evaluation Authority shall be entitled to require the sponsor to submit a fresh application for certification.

3.7 National Scheme Communications

3.7.1 The Evaluation Authority will make use of the National Scheme Communications (NSC) to provide further information, guidance, clarifications and rules for certification projects on a need basis. Each NSC will clearly mark its nature and status, whether it is for information or binding for certification projects. A NSC may be issued any time and affected certification projects will be required to comply with the NSC.

4 CERTIFICATION PRINCIPLES

4.1 For the Evaluation Authority

4.1.1 Meeting the related CCRA requirements and maintaining the corresponding status is essential for the Evaluation Authority. The following basic principles and responsibilities can be derived for the Evaluation Authority's services:

a. The certification programme of the Evaluation Authority are accessible to all interested parties[5].

b. Impartiality and objectivity are ensured and all parties are treated equally.

c. Where technical assessments are performed by independent (external) assessment bodies, equal treatment of all assessment bodies is guaranteed.

d. The interests and reservations of third parties have no bearing whatsoever on the procedures employed by the certification body and the results obtained.

[5] The certification body can refuse to accept or maintain a request for a contract to certify an applicant if there are fundamental or proven reasons, such as if the customer is involved in illegal activities, if the customer has repeatedly violated the certification or product requirements, or if there are similar problems relating to the customer.

4.1.2 The Evaluation Authority is responsible for strictly and continuously adhering to these principles and is monitored in this regard by the accreditation body[6]. The accreditation body pays particular attention to ensure that the procedures of the Evaluation Authority are accessible to all interested parties, that impartiality and objectivity are guaranteed and that all applicants are treated equally.

4.1.3 The Evaluation Authority uses and manages its marks and certificates. The Evaluation Authority monitors the use of its marks. In the event of misleading or improper use, the Evaluation Authority reserves the right to take corrective measures, make this known or, in extreme cases, take legal action.

4.1.4 If the basis on which a mark was issued ceases to apply, the Evaluation Authority shall decide whether the mark of conformity can be maintained (possibly with restrictive stipulations) or must be withdrawn (revoked). The applicant, as the holder of the mark, can also request changes or the revocation of the mark.

4.1.5 The Evaluation Authority limits its requirements, evaluations, assessments, decisions and monitoring (where necessary) to aspects that specifically and exclusively relate to the scope of application for the certification.

4.2 For the applicant

4.2.1 Upon receipt of the SCCS issued certificate, the applicant agrees to continuously adhere to the following principles:

a. The applicant always meets the certification requirements, including the implementation of corresponding changes when informed of these by the Evaluation Authority.

b. The applicant ensures that the certified product continues to meet the product requirements when the certification applies to ongoing production.

c. The applicant makes all the necessary preparations for the following:

i. Carrying out the evaluation and monitoring (where necessary), including taking account of the verification of documentation and records, access to the relevant equipment, site(s), area (s) and staff, and the applicant's subcontractors

ii. The investigation of customer complaints

[6] The accreditation body refers to the Common Criteria Management Committee (CCMC) that acts in any matters of policy relating to the status, terms and operation of the CCRA. It decides on the admittance of new participants, the compliance of new Certification Bodies, and changes to the scope of the CCRA.

iii. The participation of observers, where appropriate

d. The applicant can only make claims with regard to the certification in line with the scope of application for the certification.

e. The applicant must not use the product certification in any way that could discredit the Evaluation Authority, or make any statements about its product certification that the Evaluation Authority could consider to be misleading or unjustified.

f. When marks/certificates are issued, the currently valid version must always be used.

g. The mark/certificate must not be changed, meaning that it must be used exactly as issued by the Evaluation Authority.

h. If the certification documents, including the marks/certificates, are made available to others, the documents must be duplicated in their entirety, or as defined in the certification program.

i. If the certification is suspended, withdrawn or terminated, the use of all advertising materials that contain any reference to the certification must be ceased and the measures required by SCCS (for example, returning certification documents) as well as all other necessary measures must be taken.

j. If the certified object is referred to in communication media, such as documents, brochures or advertising materials, the requirements of the Evaluation Authority and stipulations defined in SCCS must be met. Any reference to the certified object in publicly accessible media and materials must be clear and not misleading. In particular, the certification may only be used to indicate the conformity of the certified object with the standards applied. New versions of previously certified objects may only be referred to as “certified” if a re-certification has been successfully completed and a certificate issued.

k. The Evaluation Authority must be informed immediately of any changes that could affect the ability of the applicant to meet the certification requirements[7].

l. The applicant must label products and systems as well as process-related documentation in such a way that amended versions can be

[7] Examples of changes include:
- The legal, economic or organizational status or ownership
- Organization and management (e.g., key roles, decision-making processes or technical staff)
- Changes to the product or production method
- Contact addresses and production facilities
- Significant changes to the quality management system

clearly recognized based on new version numbers, releases, etc.

m. If new security findings lead to the conclusion that a mark/certificate can no longer be justified for technical reasons, the applicant can eliminate any identified weaknesses in a reasonable time frame, document this and inform the Evaluation Authority accordingly as part of the SCCS Assurance Continuity process.

n. Records of all complaints and new findings regarding the properties of a certified object that have been made known to the applicant's customer with regard to adherence to the certification requirements must be kept and these records must be made available to the Evaluation Authority on request. In addition:

   i. The applicant must take suitable measures with regard to such complaints as well as any deficiencies that have been discovered in the products and that affect adherence to the certification requirements.

   ii. The measures taken must be documented.

o. All requirements that must be met are described in SCCS and that relate to the use of marks/certificates as well as to information relating to the product. The Evaluation Authority monitors the use of its marks/certificates. In the event of misleading or improper use, the Evaluation Authority reserves the right to take corrective measures, make this known or, in extreme cases, take legal action.

p. If necessary, the applicant must commission an external evaluation facility approved within SCCS to perform the technical evaluation.

q. The Evaluation Authority has the right to inspect any applicant documents relevant for the assessment as well as any assessment reports of the commissioned evaluation facility, insofar as this is necessary for the assessment and certification in accordance with the underlying criteria.

r. After providing notice and for the purpose of an assessment, the Evaluation Authority has the right to enter and inspect the development, testing and production sites and other facilities of the applicant, third parties commissioned by the applicant, the applicant's suppliers and other parties relevant for the assessment, insofar as this is necessary for the assessment.

4.2.2 If there is any significant failure on the part of the applicant to observe these obligations, the Evaluation Authority reserves the right to remove announcements on the SCCS website and on https://www.commoncriteriaportal.org, refuse to issue marks/certificates, and withdraw (revoke) issued marks/certificates.

5 ASSURANCE CONTINUITY

5.1 Overview

5.1.1 The purpose of Assurance Continuity (AC) is to enable developers that have made changes to their certified IT products or environmental requirements to maximise the use of previous evaluation work and maintain the same level of assurance before and after the change was made, or to get a new certificate with reduced evaluation efforts.

5.1.2 Assurance Continuity provides two alternatives, based on the nature of the changes:

a. Certificate Maintenance: may apply when effects of the changes on the assurance baseline are deemed ‘minor’

b. Re-evaluation: may apply when the effects are deemed ‘major’

5.1.3 The issue of whether the changes are minor or major is determined through a process called impact analysis. The sponsor carries out this analysis and generates an Impact Analysis Report (IAR) as result. This IAR is a key input for the Evaluation Authority to decide on the applicability of AC.

5.1.4 Assurance Continuity limits the evaluation activities to changes to certain assurance components; it therefore does not require a full evaluation as for a new product. CCRA AC provides guidelines on how to distinguish minor from major changes and the details for the IAR. However, the Evaluation Authority reserves the right to add on requirements as deemed necessary. It is recommended that the developer (and the sponsor, if applicable) familiarise itself with the latest applicable version of that document.

5.1.5 For Assurance Continuity, the following terms are used:

a. the *certified TOE* refers to the version of the TOE that has been evaluated and for which a certificate has been issued under SCCS.

b. the *changed TOE* refers to a version that differs in some respect from the certified TOE.

c. the *maintained TOE* refers to a changed TOE that has undergone the maintenance process and to which the certificate for the certified TOE also applies.

d. the *assurance baseline* refers to the culmination of activities performed by both the evaluator and developer resulting in a certified TOE.

5.1.6 To apply for Assurance Continuity, the sponsor shall submit an application

package, which consists of at least:

a. Certification Application Form (CAF);

b. Impact Analysis Report (IAR); and

c. Copy of Certificate issued under SCCS for the certified TOE.

5.1.7 Assurance Continuity depends on the validity of the assurance baseline and the previous certificate. The Evaluation Authority reserves the right not to accept a TOE for Assurance Continuity, where any grounds as stated in 6.1 for revocation of a certificate exist, or when the certificate date for the certified TOE is older than 5 years.

5.2 Certificate Maintenance

5.2.1 Maintenance refers to the process of recognising that changes made to a certified TOE are classified as 'minor' and thus have not adversely affected assurance in the TOE. This means that the assurance originally gained for the certified TOE also applies to the changed TOE. As they share the same assurance, no additional certificate will be issued. Upon successful assurance continuity, the maintenance report or the new certificate respectively will be posted on the CPL for SCCS.

5.2.2 Certificate maintenance offers the following advantages:

a. It provides a cost-effective solution to the problem of ensuring assurance continuity;

b. For a product, it enables the sponsor to improve competitiveness by reducing the time-to-market for any product updates or upgrades that do not require a re-evaluation; and

c. It allows system integrators to patch and upgrade constituent products, make minor changes to the system, and maintain assurance in a timely and cost-effective manner.

5.2.3 A changed TOE, where the change is minor, is classified as a "maintained TOE" and is given a "Maintained" status. This status indicates that the changes have not affected the assurance baseline and therefore the TOE has not been subject to any re-evaluation. The certificate for the "certified TOE" also applies to the maintained TOE.

5.2.4 A maintained TOE enjoys the same level of assurance as the original certified TOE. A risk owner can have the same confidence in a maintained TOE as in the original certified TOE. The maintained TOE will be identified as such in the Certified Products List (CPL).

5.3 Process Flow for Maintenance

5.3.1 Under the maintenance process, the Evaluation Authority interacts directly with the sponsor. However, the sponsor may choose to enlist the services of a consultant for the preparation of, or for assistance in the preparation of, the IAR.

5.3.2 When there are changes to a TOE, resulting in a new version (which typically will include a number of separate changes), the sponsor wishing to apply for certificate maintenance for the changed TOE shall provide the Evaluation Authority with an IAR with information sufficient to allow the Evaluation Authority to determine each change to be 'minor'. The IAR should show the relevant changes and the impact to the security assurance of the TOE, and provide evidence and rationale upon which the assurance of the TOE can be maintained.

5.3.3 The Evaluation Authority shall review the IAR together with other additional documents, which shall include updated evaluation deliverables from the original evaluation and certification. If the Evaluation Authority rejects the IAR (e.g. as a result of lack of evidence), the sponsor may re-submit when a revised IAR is available.

5.3.4 Where the Evaluation Authority accepts the IAR, is satisfied with the evidence provided and determines that the changes are minor, the Evaluation Authority shall update the CPL with details of the maintained TOE, such as with the new version number. The Evaluation Authority shall also generate a Maintenance Report that gives a brief summary of the changes to the certified TOE, which shall be made publicly available.

5.3.5 Where a change to a TOE is determined by the Evaluation Authority to be major, the changed TOE would have to be submitted for re-evaluation.

5.4 Re-evaluation

5.4.1 Re-evaluation refers to the process of recognising that changes made to a certified TOE are (for at least one of the changes) major and therefore require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation (in contrast to new evaluation) does not require all assurance activities to be performed as under a new evaluation, but only addresses the changes made to the previously certified TOE.

5.5 Process Flow for Re-evaluation

5.5.1 Under the re-evaluation process, the sponsor interacts with the CCTL to perform the required assurance and evaluation activities. The sponsor shall make the IAR available to the CCTL. The CCTL may request clarification or guidance from the Evaluation Authority on its assessment of the IAR.

5.5.2 The sponsor shall ensure that for each change to the certified TOE as described in the IAR, such change is clearly classified in the IAR as a

minor or major change, and the sponsor shall also ensure that the IAR includes a detailed description of each major change as well as a detailed description of the impact of each major change to the security assurance for the TOE.

5.5.3 At the end of a successful re-evaluation of the changed TOE, a new ETR is produced by the CCTL. The Evaluation Authority will issue a Certification Report and a new CC certificate. This changed TOE becomes a newly certified TOE, i.e. the updated assurance baseline for any future changes to be made.

5.6 Roles and Responsibilities under Assurance Continuity

5.6.1 Sponsor

a. The sponsor is required to submit an IAR to the Evaluation Authority, providing evidence for each change and justifying whether each change is minor or major. Any changes that affect the security assurance in the TOE will necessitate a re-evaluation. Evidence shall be provided that the changes listed in the IAR have been tested by the developer.

5.6.2 CCTL

a. The CCTL is usually not involved in the maintenance process. However, the Evaluation Authority may also request the CCTL, which was responsible for creating the assurance baseline, to assist in the review of an IAR and any additional documents.

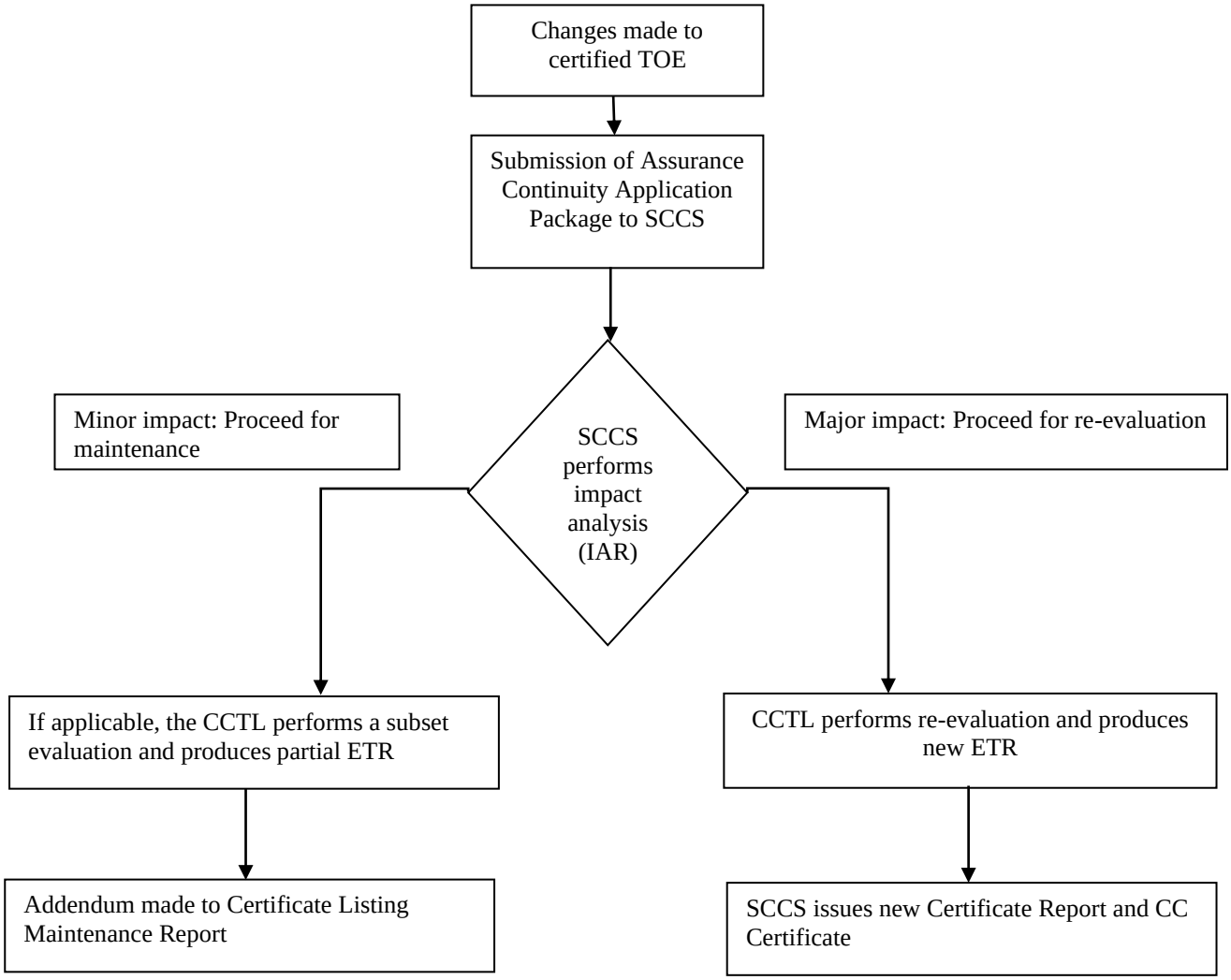
b. If a CCTL is contracted to perform a re-evaluation of a TOE, similar to the formal evaluation, the CCTL must provide the Single Evaluation Reports and a final ETR to the Evaluation Authority.

5.6.3 The Evaluation Authority

a. The Evaluation Authority reviews an IAR and any additional documents, in accordance with the requirements of the Assurance Continuity and the CCRA. If, for an application for maintenance, there is sufficient evidence that there is no major impact on the security assurance of the certified TOE and the maintenance process can successfully be applied, the Evaluation Authority grants the TOE the maintained status and updates the CPL accordingly. For a re-evaluation, the Evaluation Authority will assess whether there is sufficient evidence that re-evaluation is suitable, and if so, will accept the re-evaluation into SCCS.

b. Re-evaluation or the decision to accept certified TOE for re-evaluation under the SCCS depends on the availability of the baseline assurance from the CCTL which created it. The Evaluation Authority

reserves the right to reject an application for Assurance Continuity if required information from the CCTL is not provided or is not available for any reason.


Changes made to certified TOE
Submission of Assurance Continuity Application Package to SCCS
SCCS performs impact analysis (IAR)
Minor impact: Proceed for maintenance
Major impact: Proceed for re-evaluation
If applicable, the CCTL performs a subset evaluation and produces partial ETR
CCTL performs re-evaluation and produces new ETR
Addendum made to Certificate Listing Maintenance Report
SCCS issues new Certificate Report and CC Certificate

6 REVOCATION, SUSPENSION, WITHDRAWAL AND TERMINATION

6.1 Revocation of Certificates

6.1.1 The Evaluation Authority is entitled to revoke a CC certificate issued under SCCS forthwith if:

a. The CCTL, sponsor or developer is in breach of any terms of SCCS Publications, the CAF and/or any other terms as agreed to in writing with the Evaluation Authority (collectively the “SCCS Terms”);

b. The sponsor or developer has failed to disclose any known or discovered vulnerabilities that, in the Evaluation Authority’s opinion, can undermine the CC certification;

c. The sponsor or developer fails to take any corrective measures during the period of grace given by the Evaluation Authority to the satisfaction of the Evaluation Authority;

d. The sponsor or developer misuses the certification status, CC certificate or any proprietary names and marks associated with CSA, the Evaluation Authority, SCCS, CCRA or CC;

e. The sponsor or developer makes any statement that misrepresents any aspect of evaluation or the effect of any certification under the SCCS;

f. The Evaluation Authority finds that the CCTL was in a position of conflict that impaired its ability to conduct a fair and impartial evaluation of the TOE;

g. The TOE relies heavily on the IT environment to meet its specified security objectives, and the IT environment is no longer able to meet its required security objective;

h. The certified TOE no longer meets the conditions under which certification was granted or does not meet any changed conditions for certifications introduced by the Evaluation Authority after the TOE was originally certified.

6.1.2 Upon the revocation of a CC certificate, the sponsor, developer (where the developer is not the sponsor) and the CCTL shall immediately cease all use of the CC certificate or any proprietary names and marks associated with CSA, the Evaluation Authority, SCCS, CCRA, or CC and desist from holding the applicable products out as being certified under the SCCS.

6.1.3 The Evaluation Authority will inform the sponsor, developer (where the developer is not the sponsor) and the CCTL in writing of the revocation of the CC certificate, and will remove the listing of the certified product (TOE) from the Certified Product List (CPL). The project details will be put into the common Historical Product List (HPL).

6.1.4 Revocation of a certificate will automatically extend to all maintained and re-evaluated TOEs, which are based on the revoked certificate. This applies even if the reasons for revocation of a certificate may have been addressed during maintenance or re-evaluation, because revocation of the certificate equates to revocation of the assurance baseline.

6.2 Suspension and Termination of On-Going Projects

6.2.1 For the purposes of 6.2, the term “on-going certification procedure” means a procedure for certification under SCCS or a procedure for Assurance Continuity and such a procedure is deemed to have commenced upon the submission by the sponsor of the relevant application package to the Evaluation Authority.

6.2.2 The Evaluation Authority is entitled to terminate an on-going certification procedure without issuing a certificate at any stage forthwith by notice in writing to the sponsor if:

a. The sponsor/developer has not paid any sums due to Evaluation Authority in respect of the certification project;

b. No evaluation or certification activity has taken place for more than 60 consecutive calendar days;

c. A CCTL or sponsor fails to take any action within the requisite timeframe in an EWP, an OR or otherwise stated by the Evaluation Authority, and has not obtained the approval of the Evaluation Authority and (where applicable) the other party (be it the CCTL or sponsor) to a revised timeframe;

d. The progress of the evaluation has deviated from the EWP by more than 50%. For instance, the proposed effort for ADV evaluation is four (4) weeks and it is still not completed after six (6) weeks;

e. The scope of evaluation changes such that the product under evaluation no longer fulfils the requirements for admittance into the scheme;

f. Severe security flaw is discovered in the product during the course of evaluation and resolution of the security flaw requires extensive re-engineering or causes significant delay to the project completion date. In addition, the Evaluation Authority may terminate the project if the resolution is deemed insufficient (i.e. high residual risks) or inappropriate;

g. A sponsor or a CCTL has suspended or terminated a project in accordance with the terms of the contract entered into between them. In that event, the party that has suspended or terminate the project shall notify the Evaluation Authority in writing of the suspension or termination within seven (7) calendar days thereof;

h. The CCTL's quality of work or intermediate reports is/are repeatedly insufficient, the Evaluation Authority requires frequent corrections, and/or the CCTL fails to meet deadlines as outlined in the EWP;

i. The sponsor's submissions repeatedly fail to address corrective actions, to provide required clarity, and/or fail to meet deadlines as outlined in the EWP.

6.2.3 The Evaluation Authority may also suspend or terminate an on-going certification procedure under the SCCS for reasons given in 6.1.1 above by giving written notice to the sponsor. Suspension means that the Evaluation Authority will mark the project as suspended in the website, and may allocate its resources to other projects. Suspension can apply for the same reasons as termination, but may also apply in cases where the developer and CCTL need to change the EWP due to findings or other reasons for project delay, and where the updated EWP cannot be established within 30 calendar days after the Evaluation Authority has requested a new version of the EWP from the CCTL. Suspension aims to allow the developer to focus on issues of evaluation and/or planning without the need for the Evaluation Authority to keep resources allocated. The certification procedure can resume after the Evaluation Authority has sufficient evidences that the EWP can be achieved and has the same or equivalent resources available as before suspension.

6.2.4 The Evaluation Authority may consult with the CCTL and sponsor to confirm the status of the project before proceeding to inform them in writing of the decision to terminate the certification procedure.

6.2.5 Upon the termination of a certification procedure under the SCCS, the Evaluation Authority will close its file and the Evaluation Authority resources assigned to the project will be released. Where the certification procedure relates to evaluation for CC certification, the Evaluation Authority will remove the TOE from the "Product in Evaluation" list (EPL). The certification procedure details will be put into the common Historical Project List (HPL), marked as 'terminated'. Where the certification procedure relates to assurance continuity, the Evaluation Authority will not update the CPL or the status of the TOE.

6.3 Withdrawal from On-Going Certification Procedures

6.3.1 Where a sponsor wishes to terminate its appointment of a CCTL and wishes to engage another CCTL to continue a certification procedure under the SCCS, such replacement shall be subject to the prior written

approval of the Evaluation Authority and on such terms and conditions as the Evaluation Authority shall deem fit. The Evaluation Authority reserves the right to reject a replacement of CCTLs and to require the sponsor to re-apply to the Evaluation Authority and go through a fresh evaluation and certification process.

6.3.2 When a sponsor wishes to withdraw an ongoing certification procedure, the CCTL, the developer (where the sponsor is not the developer) and the Evaluation Authority shall be informed in writing by the sponsor. The arrangement between the CCTL and the sponsor are part of the contractual agreement between those parties. The sponsor shall however, independently of the agreement or arrangement with the CCTL, inform the Evaluation Authority in writing 2 weeks before the withdrawal can become effective. The certification procedure indication will be removed from the EPL by the Evaluation Authority and the project details will be put into the common Historical Project List (HPL), marked as 'withdrawn'.

6.3.3 A CCTL or a developer (where the developer is not the sponsor) cannot withdraw a certification procedure. Only a sponsor can withdraw an ongoing certification procedure. However, nothing in this SCCS Publication #3 prevents a CCTL from withdrawing from a certification procedure. The CCTL's right to withdraw from a certification procedure is subject to the terms of the agreement between the CCTL and the sponsor. The CCTL shall give the sponsor and Evaluation Authority advanced written notice of any withdrawal from a certification procedure. Upon the withdrawal of the CCTL from a certification procedure, the sponsor may decide to try to continue the project with another CCTL, or withdraw the project. The sponsor shall inform the Evaluation Authority of its decision in writing and obtain the Evaluation Authority's approval of the replacement CCTL within such time as the Evaluation Authority shall specify, failing which the certification procedure shall be deemed withdrawn from the SCCS. The certification procedure will then be removed from the EPL by the Evaluation Authority and the certification procedure details will be put into the common Historical Project List (HPL), marked as 'withdrawn'.

6.4 Survival

6.4.1 Any obligations of a sponsor or CCTL under the SCCS or their respective agreements with the Evaluation Authority which by their nature would continue beyond termination or expiration thereof, including without limitation the obligations set out in 7, 9, 10 and 12 of the SCCS Publication #3, shall survive such termination or expiration.

6.5 No refund of fees

6.5.1 Upon withdrawal, suspension, or termination of a certification procedure, there will be no refund of any fees or payments received by the Evaluation Authority, and no demands or claims shall be made against

the Evaluation Authority in connection with such withdrawal, suspension or termination of the certification procedure. Outstanding payments, e.g. for overseas site-visit by the Evaluation Authority, shall become immediately due and payable by the sponsor. To subsequently obtain certification of the same IT product or PP, a sponsor must re-apply to the Evaluation Authority and go through a fresh evaluation and certification process.

7 INFORMATION PROVIDED BY/TO THE EVALUATION AUTHORITY

7.1 Public Information

7.1.1 CSA maintains a public website that contains a broad range of information about the SCCS as well as information that CSA is required under the CCRA to publish. In compliance with the CCRA, CSA shall publish the CPL, containing particulars of the TOEs evaluated within the SCCS which hold a currently valid CC certificate. Documents that will be made publicly available include a copy of the CC certificate, the ST, PP (if applicable) and CR of those TOEs and Maintenance Reports.

7.1.2 The purpose of publication is to facilitate mutual recognition as described in SCCS Publication #1. The information informs the public of the evaluated products that are available, and provides a source of reference for users to verify the current status of issued certificates.

7.2 Confidential Information

7.2.1 The sponsor or the CCTL (as the case may be) shall review and confirm promptly in writing the release of information by the Evaluation Authority before it is made available to the public. Such confirmation shall be provided within the time stipulated by the Evaluation Authority, failing which the information may be released by the Evaluation Authority free from any obligation of confidentiality.

7.2.2 It is the responsibility of the sponsor and the CCTL (as the case may be) to ensure that any information published by the Evaluation Authority does not contain any proprietary or protected information.

7.2.3 If a sponsor does not wish to have a TOE included in the EPL and CPL or otherwise made available to the public, it must notify the Evaluation Authority as part of the CAF. A TOE that is not listed on the CPL will not be eligible for mutual recognition under the CCRA.

7.2.4 Any information that is not publicly releasable must be explicitly marked or labelled as such by the sponsor or the CCTL (as the case may be) before being delivered to the Evaluation Authority.

7.2.5 Notwithstanding any of the above, the Evaluation Authority will not be

liable for the disclosure of information designated as confidential or proprietary if the Evaluation Authority determines that withholding the information is contrary to law or its obligations under the CCRA.

7.2.6 Except with the written consent of the Evaluation Authority, the sponsor and the CCTL shall not disclose to any person any information, documents or materials provided by the Evaluation Authority where the same has not been made publicly available by CSA ("Evaluation Authority Confidential Information").

7.2.7 The sponsor and the CCTL shall not, without the prior written consent of the Evaluation Authority make use of any Evaluation Authority Confidential Information other than for the purposes of the project for which the Evaluation Authority Confidential Information was disclosed to them.

7.2.8 The sponsor and the CCTL shall keep confidential the Evaluation Authority Confidential Information and shall only disclose it to their employees on a need to know basis for the purposes of the project for which the Evaluation Authority Confidential Information was disclosed. Without prejudice to the generality of the foregoing, no Evaluation Authority Confidential Information shall be stored or distributed by the sponsor or CCTL outside its local protected IT infrastructure. The sponsor and the CCTL each undertakes to take such steps as shall be necessary to protect the Evaluation Authority Confidential Information and to notify the Evaluation Authority as soon as it becomes aware of any unauthorised use of the whole or any part of the Evaluation Authority Confidential Information.

7.2.9 All documents and other materials containing the Evaluation Authority Confidential Information shall, at the Evaluation Authority's request, be returned or otherwise disposed of in the manner specified by the Evaluation Authority.

7.3 Proprietary Information

7.3.1 Nothing in this document shall affect any person's ownership rights in and title to that that person's pre-existing Intellectual Property (IP) or IP independently brought into existence or acquired by that person without reliance on any SCCS/CC IP. The term "IP" is defined in 10.3 below. All documents and other materials provided by the Evaluation Authority to the sponsor or CCTL shall remain property of CSA and shall at the Evaluation Authority's request be returned to the Evaluation Authority or disposed of in the manner specified by the Evaluation Authority.

7.3.2 The sponsor and the CCTL acknowledges and agrees that the Evaluation Authority shall have the right to use, reproduce, format, modify, and create derivative works of the IP that it provides to the Evaluation Authority, and to allow third parties to do so, all in the manner set out in SCCS Publications and the CCRA.

7.3.3 Before delivering any IP to the Evaluation Authority, the sponsor and the CCTL shall ensure that it owns or has all the necessary right, power and authority to disclose such IP to the Evaluation Authority and to allow the Evaluation Authority to exercise its rights as stated in 7.3.2.

7.3.4 Before requesting for the evaluation or assurance maintenance of a TOE under the SCCS, each sponsor shall ensure that it owns the TOE or has all the necessary right, power and authority to make such a request and to fulfil the role of a sponsor of the TOE.

7.3.5 The sponsor and the CCTL shall, if required by the Evaluation Authority, do all acts and execute or procure the execution of such documents as may reasonably be required in order to perfect, protect or enforce any of the Evaluation Authority's rights hereunder to the IP provided by sponsor or the CCTL.

7.4 The Developer

7.4.1 Where the sponsor is not the developer, all the obligations of the sponsor under 7 shall also apply equally to the developer.

8 MUTUAL COOPERATION

8.1.1 The sponsor and CCTL shall each adhere to the timeframes set out in the EWP (where applicable) or otherwise approved by the Evaluation Authority for the performance of their respective obligations in relation to evaluations under the SCCS or (where applicable) activities under the Assurance Continuity.

8.1.2 The sponsor and CCTL shall provide each other and the Evaluation Authority, as applicable, with such information, documentation and materials as they shall each require with reasonable promptness and attend such meetings with each other and/or the Evaluation Authority as required from time to time.

8.1.3 The sponsor and CCTL shall, as applicable, co-operate with each other and the Evaluation Authority in order to fulfil their respective obligations under the SCCS in a timely and efficient manner.

8.1.4 The sponsor and CCTL shall, as applicable, co-operate with the Evaluation Authority in any promotional activities for the SCCS undertaken by the Evaluation Authority and render such support and assistance as the Evaluation Authority may reasonably require from time to time.

8.1.5 If the sponsor is not the developer of the IT product, the sponsor shall be solely responsible for ensuring the developer's co-operation with the CCTL and Evaluation Authority on all matters relating to the developer's

product, ST/TOE or PP, the developer's attendance at the TKM and all other meetings called by the Evaluation Authority or CCTL, and the developer's performance of all tasks assigned to it by the sponsor, CCTL or the Evaluation Authority. The sponsor and CCTL shall co-operate in making all necessary arrangements directly with the developer for the production and submission of any documents or information to the Evaluation Authority and for the disclosure and use of such documents and information by sponsor, developer and CCTL.

9 CONFLICTS OF INTEREST

9.1 General Obligation to Avoid Conflicts of Interests

9.1.1 As noted above, the sponsor or developer (if sponsor and developer are different parties) may hire a CCTL to provide advice, assistance and consultancy services in the course of preparing for an evaluation under the SCCS or an IAR for Assurance Continuity. Such services may include reviewing and preparing evaluation evidence, assisting in resolving evaluation issues, assisting the sponsor in performing the impact analysis and documenting the results in an IAR. As used in this section, the term "consultancy services" shall refer to the services described in this paragraph.

9.1.2 Hiring a CCTL to provide consultancy services is not strictly required, nor is the Evaluation Authority involved in any party's decision to do so. The scope of the consultancy services is a matter for negotiation between the CCTL and the party hiring it for such consultancy services.

9.1.3 Where a CCTL is hired to provide any consultancy services, such consultancy services may also result in a future conflict of interest should the same CCTL serve as the evaluator for a future evaluation of the changed TOE.

9.2 Duty to Disclose Conflict of Interests

9.2.1 For each evaluation under the SCCS, the CCTL shall notify the Evaluation Authority of any known or potential conflict of interests relevant to that evaluation.

9.2.2 The Evaluation Authority will determine whether a conflict of interest exists on a case-by-case basis. The Evaluation Authority is the final arbiter in determining whether a potential or actual conflict of interest exists and whether the CCTL should or should not participate in the evaluation under the SCCS.

9.3 Conflict of Interest Guidelines

9.3.1 The guidelines in this section are intended to assist CCTLs that provide consultancy services to avoid conflict of interest situations, but are not

exhaustive.

9.3.2 The CCTL shall not accept for evaluation any product developed, manufactured, or sold by an entity that possesses an ownership interest in the CCTL or in which the CCTL has an ownership interest. The term “ownership interest” shall include any percentage of ownership which is greater than 5%.

9.3.3 The CCTL must not have entered into an agreement that would result in the CCTL directly benefiting financially from commercial sales of the product being evaluated or in which the CCTL has sole distributorship for the evaluated product.

9.3.4 Neither the CCTL nor its parent company, affiliates or any individual CCTL staff member concerned with a particular evaluation shall have a vested interest in the outcome of that evaluation.

9.3.5 A CCTL staff member or evaluation team member cannot, under any circumstances:

a. Providing both consultancy and evaluation services for the same TOE, regardless of whether in his/her official or personal capacity;

b. Be concurrently employed/appointed in another unit of the organization or another organization which develops IT Product(s);

c. Own shares of organization which develops IT Product(s); and

d. Develop IT Product(s) for public circulation (e.g. open source) or commercial purposes.

9.3.6 The CCTL must ensure that there is sufficient separation of control and influence in order that its parent company or affiliates cannot exert undue influence on the outcome of evaluation activities and proprietary or confidential evaluation information cannot be inappropriately accessed by its parent company or affiliates.

9.3.7 The role of consultancy and evaluation must be clearly separated at all times.

9.3.8 The CCTL shall only use the evaluators as named in the EWP and approved by the Evaluation Authority. Any changes to the evaluator team must be communicated and approved by the Evaluation Authority in advance. In addition, any new staff assigned to the project and approved by the Evaluation Authority must submit an additional declaration of not having any conflict of interest in the project. A director of the CCTL or such other person in a similar capacity with authority to bind the CCTL must also provide a declaration that such new staff are not in a position of conflict. For the original team, no separate declaration is required, as the CAF already requires such a declaration from the CCTL for the

nominated staff of the project.

10 INTELLECTUAL PROPERTY

10.1 SCCS/CC/CCRA IP

10.1.1 The entire right, title and interest (including without limitation intellectual property rights) in and to any and all trademarks and logos of the Evaluation Authority and SCCS (the "SCCS Marks"), CC certificates and other IP (defined below) provided by or obtained from CSA (collectively the "SCCS/CC IP") belong to CSA and/or its licensor(s).

10.1.2 The sponsor and developer may use the CC certificate and such SCCS Marks as the Evaluation Authority may specify in writing from time to time strictly for the purpose of indicating that the product named in the certificate has been evaluated and certified under the SCCS using the CC at the designated assurance level.

10.1.3 A CCTL may use such SCCS Marks as CSA may specify in writing from time to time strictly for the purpose of indicating that the CCTL has the approval of CSA to conduct IT security testing and evaluation in Singapore under the SCCS using the CC at the designated assurance level.

10.1.4 Any goodwill generated by the use of the SCCS Marks shall accrue to CSA and its licensor(s).

10.1.5 Any rights granted to use any SCCS/CC IP are personal to the sponsor, developer and CCTL. The sponsor, developer and the CCTL shall not grant sub-licences to or otherwise authorise any third party or otherwise assign its right to use the SCCS/CC IP for any purpose whatsoever.

10.1.6 The sponsor, developer and CCTL shall immediately discontinue the use of the SCCS/CC IP and return to CSA or destroy all materials bearing SCCS/CC IP upon written notice by CSA.

10.1.7 Notwithstanding anything to the contrary in the SCCS Terms, all use of the SCCS/ CC IP is subject to the terms and conditions of the CCRA and any documents issued pursuant to the CCRA.

10.2 SCCS/CC IP Guidelines

10.2.1 Sponsors, developers and CCTLs shall comply with any applicable guidelines in the SCCS Publications or issued by CSA from time to time regarding their use of any of the SCCS IP.

10.3 IP

10.3.1 In this document, "IP" means any ideas, data, inventions, discoveries,

developments, enhancements, works of authorship, programs, and technical, business and other information and any property rights protected under the patent, copyright, mask work rights, trade secret, trademark or other intellectual property or moral rights law of any state or national government including all rights under any registrations issued by any governmental authority with respect to the said ideas, data, inventions, discoveries, developments, enhancements, works of authorship, programs, and technical, business and other information, and the said property rights as well as all rights under any pending applications for registration and any applications for registration.

11 FEES

11.1 General Policy

11.1.1 The fees for CSA's work in connection with the certification process shall be prescribed by CSA and published on the CSA website. CSA reserves the right to review the fees as and when necessary. These costs are based primarily on the type of procedure requested, the specific object to be certified, the scope of certification desired and the degree of assessment envisaged or required. However, the procedure costs are charged irrespective of the ordering party's attributes (company name, company size, registered office, division, etc.).

11.1.2 All fees are in Singapore dollars and are subjected to GST.

11.1.3 Certification fees are always charged as agreed – regardless of whether a mark/certificate has been issued or could not be issued due to technical deficiencies or other deficiencies, the applicant cancelled the procedure or the Evaluation Authority suspended the procedure due to failure to provide the necessary information.

11.1.4 If the sponsor requires modifications to reports, expert opinions or marks/certificates that CSA has already approved, the additional effort will be charged to the sponsor. This also applies to performing re-assessments, if these become necessary due to reasons caused by the sponsor.

12 LIABILITY

12.1 Disclaimer

12.1.1 CSA makes no representations, warranties or covenants of any kind, whether express, implied or statutory, with respect to the SCCS, SCCS/CC IP, CCTLs, or any evaluations conducted or certifications awarded under the SCCS, including without limitation any warranties of merchantability, satisfactory quality, fitness for a particular purpose or non-infringement of third party rights and any warranties that they are

accurate, reliable or error-free. All implied warranties of any kind are excluded to the maximum extent permitted by law. Any person's use of and/or reliance on the SCCS, CC IP, CCTLs, or evaluations conducted or certifications awarded under the SCCS shall be at their own risk.

12.1.2 To the extent permissible by law, in no event will CSA, its officers, directors, employees or any other person acting under the direction of CSA be liable to a sponsor, developer, CCTL or any other person for any loss or damage under any theory of liability, whether direct, indirect, incidental, special, consequential or exemplary in nature, arising out of or in connection with the SCCS or any decisions by CSA or any such person in relation to the SCCS if made in good faith in the ordinary course of the discharge of the CSA's duties under the SCCS, including but not limited to lost profits, loss of goodwill and business opportunities, costs of procurement of substitute goods or services, business interruption or loss of business information and data, even if the CSA has been advised of the possibility of such damages.

12.2 Indemnity

12.2.1 To the extent permissible by law, each sponsor shall indemnify, defend and hold harmless and release CSA and its agents, directors, officers, employees, successors, assigns and representatives thereof (collectively the "Releasees") from and against any and all claims, demands, suits, actions, judgments, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the sponsor under SCCS Terms, any act, neglect or omission by the sponsor/ or its agents, directors, officers, employees, successors, assigns and representatives and/or any dispute between the sponsor with a CCTL or a developer or any other third party arising out of or in connection with the foregoing or the SCCS.

12.2.2 To the extent permissible by law, each CCTL shall indemnify, defend and hold harmless and release CSA and its agents, directors, officers, employees, successors, assigns and representatives thereof (collectively the "Releasees") from and against any and all claims, demands, suits, actions, judgments, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the CCTL under the SCCS Terms, any act, neglect or omission by the CCTL or its agents, directors, officers, employees, successors, assigns and representatives and/or any dispute between the CCTL and a sponsor or a developer or any other third party arising out of or in connection with the foregoing or the SCCS.

12.2.3 To the extend permissible by law, each developer shall indemnify, defend and hold harmless and release CSA and its agent, directors, officers, employees, successors, assigns and representatives thereof (collectively the "Releasees") from and against any and all claims, demands, suits,

actions, judgements, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the developer under the SCCS Terms, any act, neglect or omission by the developer or its agent, directors, officers, employees, successors, assigns and representatives and/or any disputes between the developer with a sponsor or a CCTL or any other third party arising out of or in connection with the foregoing or the SCCS.

13 USE OF PROTECTIVE MARKS, LOGOS AND ADVERTISEMENT

13.1 Advertisement and promotion of certified products

13.1.1 Proper and appropriate use of marks/certificates is contractually imposed on the applicant, see 4.2 above.

13.1.2 Applicants are to refer to Annex E of the "*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014*, for the terms and conditions on the use of the Common Criteria Certification Mark and the Recognition Arrangement Service Mark.

13.1.3 These guidelines apply to the following mark (the "SCCS Mark"):

13.1.4 The SCCS Marks may be used by a sponsor in conjunction with advertising, marketing, and selling of its products, where such products have successfully completed evaluation under the SCCS, have been issued a CC certificate by CSA and are listed on the CPL. The mark indicates the basic assurance level only and does not include all augmentation items. The '+' symbol may be used to indicate augmentation in general (e.g. "EAL2+").

13.1.5 The certified product name and specific version number, as listed on the CPL, must be included in any product packaging or publicity materials in which the SCCS Mark also appears.

13.1.6 Where any product packaging or publicity material refers to the certified product and to other products, the layout of information relating to the products relative to the position of the SCCS Mark should not be used in a manner that would or would likely mislead the public into thinking that a product is certified under the SCCS when in fact it is not.

13.1.7 In relation to product displays, the SCCS Mark should be displayed near the certified product or its replica or image in a manner that makes it clear that the SCCS Mark refers to the certified product.

13.1.8 The SCCS Mark must be used in the form depicted above. It shall not be altered in any way except for size and monochromatic colour schemes.

13.1.9 CSA reserves the right to require the sponsor and the developer to submit samples of their proposed use of the SCCS Mark for prior approval.

13.1.10 The following statement should appear together with any instance of use or display of the SCCS Mark:

"Official mark of the Singapore Common Criteria Scheme (SCCS), used only by Common Criteria (CC) certificate holders under license.

Conditions for CC certification can be found at [https://www.csa.gov.sg/programmes/csa-common-criteria/csa-cc-publications]

13.1.11 The following are examples of acceptable promotional language that can be used in conjunction with the advertising, marketing, and sale of a product for which the certificate is issued:

"Certified in compliance with the SCCS [Assurance Level]"

"[certified product name and version number] by [developer] has been certified under the Singapore Common Criteria Scheme to meet the [Assurance Level] for Common Criteria requirements. Conditions for Certification can be found at [https://www.csa.gov.sg/programmes/csa-common-criteria/csa-cc-publications]"

"[certified product name and version number] by [developer] has been certified under the terms of the Singapore Common Criteria Scheme. Conditions for Certification can be found at [https://www.csa.gov.sg/programmes/csa-common-criteria/csa-cc-publications]"

"[certified product name and version number] by [developer] has been listed as a Certified Product List maintained by Cyber Security Agency of Singapore under the Singapore Common Criteria Evaluation and Certification Scheme. Conditions for Certification can be found at [https://www.csa.gov.sg/programmes/csa-common-criteria/csa-cc-publications]"

13.1.12 As shown above, all promotional language must include a statement to inform the audience of the web site address [https://www.csa.gov.sg/programmes/csa-common-criteria/csa-cc-publications] at which the conditions of certification under the SCCS can be found.

13.1.13 Certification under the SCCS merely indicates that a product meets with specifically identified criteria under the CC. It is not a guarantee or assurance by CSA or an assumption by CSA of any responsibility toward any person of the quality of the product or effects of using the product. Sponsors, developers and CCTLs must avoid making statements that indicate this or may give this impression.

13.1.14 The following are examples or unacceptable promotional language:

"[Developer or its product or service] is endorsed/ recommended/ approved/ sponsored/supported/ guaranteed by the Cyber Security Agency of Singapore"

"[Developer or its product or service] is under a guarantee/warranty by the Cyber Security Agency of Singapore"

13.1.15 A sponsor or developer may reproduce a CC certificate to promote the fact that its product as named in the certificate is certified so long as the entire CC certificate is visible and is not altered in any way expect for size and monochromatic colour schemes.

13.1.16 Where any product packaging or publicity material refers to the certified product and to other products, the layout of information relating to the products relative to the position of the CC certificate should be decided with care. In all cases, the CC certificate should not be used in a manner that would or would likely mislead the public into thinking that a product is certified under the SCCS when in fact it is not.

13.1.17 In relation to product displays, the CC certificate should be displayed near the certified product or its replica or image in a manner that makes it clear that the CC certificate refers to the certified product.

13.1.18 For general information about the use of the SCCS Mark and promotion of products certified under the SCCS, please contact the Technical Manager of SCCS.

13.2 Monitoring the use of marks/certificates

13.2.1 Monitoring of the use of marks/certificates within SCCS involves the following:

a. Limiting the validity of marks/certificates to a maximum of five years with the possibility of a full assessment to determine whether the underlying certification decision can be maintained.

b. Performing an event-based assessment to determine whether the underlying certification decision can be maintained. Such an event may, for example, be a security-related problem that has become known in the specific object of certification or the relevant technology.

13.3 Response to Misuse

13.3.1 Any misuse of SCCS Marks or CC Marks shall, without prejudice to any other rights and remedies of CSA or its licensor(s), entitle CSA to take any or all of the following actions:

a. CSA will inform the relevant party to adopt the correct use;

b. CSA will remove all reference and material from the SCCS website mentioning the affected product or certificate;

c. CSA will request the removal of all reference and material from the CCRA portal (www.commoncriteriaportal.org) website mentioning the

affected product or certificate;

d. CSA will publish on its website a note regarding any misuse.

13.3.2 Any false, misleading or improper statement about the SCCS shall, without prejudice to any other rights and remedies of CSA or its licensor(s), entitle CSA to take any or all of the following actions:

a. CSA will inform the relevant party to correct such false, misleading or improper statements about the SCCS;

b. CSA will publish on its website a note regarding any misuse.

14 REFERENCES

[1] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 17025:2017 *General requirements for the competence of testing and calibration laboratories.*

[2] Singapore Accreditation Council. *Accreditation Process, SAC-Singlas 001.* March.

[3] Singapore Accreditation Council. *General Requirements for the Accreditation of Information Technology Security Testing Laboratories, IT 001.* Singapore, April 2018.

[4] Singapore Accreditation Council. *Laboratory Assessment Checklist.* Singapore, April 2018.

[5] SCCS Publication 1 – *Overview of the Scheme.* Version 8.0, June 2024

[6] SCCS Publication 2 – *Requirements for CCTL.* Version 8.0, June 2024

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

[8] Common Criteria for Information Technology Security Evaluation – Part 1: *Introduction and general model*. November 2022 CC:2022 Revision 1.

[9] Common Criteria for Information Technology Security Evaluation – Part 2: *Security functional components*. November 2022 CC:2022 Revision 1.

[10] Common Criteria for Information Technology Security Evaluation – Part 3: *Security assurance components*. November 2022 CC:2022 Revision 1.

[11] Common Criteria for Information Technology Security Evaluation – Part 4: *Framework for the specification of evaluation methods and activities*. November 2022 CC:2022 Revision 1.

[12] Common Criteria for Information Technology Security Evaluation – Part 5: *Pre-defined packages of security requirements*. November 2022 CC:2022 Revision 1.

[13] Common Methodology for Information Technology Security Evaluation – *Evaluation Methodology.* November 2022 CEM:2022 Revision 1.

[14] Assurance Continuity – *CCRA Requirements*. June 2012 Version 2.1

ACRONYMS

The following acronyms are used in CSA Publication 1,2 and 3:

AC	Assurance Continuity
SER	Single Evaluation Report
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CCRA	Common Criteria Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Evaluation Methodology
CAF	Certification Application Form
CPL	Certified Product List
CR	Certification Report
CSA	Cyber Security Agency of Singapore
EAL	Evaluation Assurance Level
EPM	Evaluation Progress Meetings
ETR	Evaluation Technical Report
EWP	Evaluation Work Plan
FIPS	Federal Information Processing Standards
IAR	Impact Analysis Report
IP	Intellectual Property
MC	Management Committee
OR	Observation Report
PP	Protection Profile
RR	Review Report

SAC	Singapore Accreditation Council
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria evaluation and certification Scheme
SFR	Security Functional Requirement
SMT	Senior Management Team
ST	Security Target
TKM	Task Kick-off Meeting
TOE	Target of Evaluation

Annex A

Task Kick-Off Meeting (TKM) Agenda

Certification ID: XXXXXX

The Task Kick-Off Meeting (TKM) should cover:

1 Evaluation Authority

a. To outline the objective of the meeting.
b. To review/adjust meeting agenda if necessary to accommodate any changes.
c. To introduce the members of the sponsor, the CCTL and the Evaluation Authority team who are involved in the evaluation and certification work.
d. To identify the point-of-contacts including the Scheme Manager, Technical Manager and Certifiers involved in the certification work.
e. To provide a brief description of the SCCS scheme.
f. To provide a brief description of the certification process and the roles played by each party in the SCCS.
g. To give an overview of the Certification Plan.
h. To outline the objectives, expectations, limitation and issues.
i. To review the scheduled activities/meetings.

2 Sponsor (and Developer)

a. To identify the point-of-contacts who are involved in the evaluation work.
b. To provide a brief description of the IT product or PP.
c. To explain the objectives, expectations and desired completion schedule of the evaluation and certification work.
d. To highlight the copyright and ownership of documents generated during the evaluation and certification including, but not limited to SER, OR and ETR.
e. To identify a scheduled day to conduct training on the IT product for the staff members of the Evaluation Authority and the CCTL involved in the evaluation and certification work.

3 CCTL

a. To identify the point-of-contacts who are involved in the evaluation work.
b. To provide a brief description of the EWP.
c. To explain the scope of evaluation and the evaluation timeline.
d. To outline the objectives, expectations, limitation and issues.
e. To schedule relevant dates, frequency and venue for EPM.

f. Applicability of Supporting Documents to the project.

4 Overseas Travel Requirements

To address overseas travel requirements for the Evaluation Authority, e.g. to attend site-visits, testing or vulnerability penetration testing by the CCTL.

5 Any Other Business

To discuss any miscellaneous topics raised by any of the members.

5 Meeting wrap-up

The Evaluation Authority will make closing remarks, action items, meeting summary, and review of key points/schedules, etc.

Annex B

Evaluation Progress Meeting (EPM) Agenda

Certification ID: XXXXXX

The Evaluation Progress Meeting (EPM) should cover:

1 Introduction

The Introduction outlines objectives of the meeting, a brief description of the progress of the TOE evaluation and any issues that arise during the evaluation process.

2 Minutes of previous minutes

3 Matters arising from previous meeting

4 Evaluation progress and milestones

This outlines the latest progress and development of the evaluation work being performed and compares them against the milestones in the Evaluation Work Plan (EWP).

5 Evaluation issues

This describes any problem encountered during the evaluation process. The issues can be related to the quality, inaccuracy and insufficiency of the deliverables provided by the sponsor, the raise of the Observation Report (OR) for a failure of any work units, the status of the last OR, changes of staff in CCTL which have an impact on the evaluation work, time schedules, etc.

6 Summary of action items

This summarises the list of action items to be completed, by who and when.

7 Arrangement for next meeting

This specifies the date, time and venue of next meeting.

Annex C

Single Evaluation Report (SER) Format

Certification ID: XXXXXX

The Single Evaluation Report (SER) should include:

1 Introduction

a. General Description

The section specifies the evaluation activity, e.g. Assurance Development (ADV) in relation to the TOE being evaluated.

b. Structure, References and Terminology

This section describes the structure of the document. It also highlights the references, *e.g.*, CC Part 2, CC Part 3 and CEM being used for production of this report. The terminology and explanation used will also be included in this report.

c. Inputs and Methods

The inputs refer to all input references and evaluation deliverables, e.g. the ST or PP, Admin Manual, User Manual, Installation Manual, and so on, used in the evaluation of this activity.

The methods refer to the procedures and/or processes used to evaluate the activity and/or its sub-activity, in accordance with the CEM. Details of such work must be recorded in the evaluator's logbook.

Table C.1: Sample Inputs Reference Table

SER Issue Number	Input References
1.0	ST v1.2 Admin Manual v1.1 User Manual v1.1 Installation Manual v1.1 CC Part 3

2 Results

The Results section should cover:

a. Summary

The summary specifies the activity description and verdict down to Work Unit Level.

This section contains the verdicts given by the evaluator for the activity, e.g. for ADV, a relevant sub-activity is ADV_FSP.1. The relevant sub-activities at action and work unit level are for example ADV_FSP.1.1E, ADV_FSP.1.2E, etc. There are only three verdicts for SER: Pass, Fail or Inconclusive.

Table C.2: Sample of the Activity Verdict Table

Activity Verdict Table	
Author:	
Start Date:	
End Date:	
Reference No.:	
Activity:	ADV
Verdict:	Pass
Summary:	
Sub-activity	**Verdict**
ADV_FSP.1	Pass

Table C.3: Sample of the Sub-Activity Verdict at Work-unit Level Table

Action/work unit	**Verdict**	**OR Raised**	**Comments**
ADV_FSP.1.1E	Pass		
1-1	Pass		
1-2	Pass		
1-3	Pass		

b. **The Evidence Summary**

This section presents a summary of the evidence and the justifications that supports the evaluators' verdicts for each individual work unit. Below is an example of evidences required for each assurance level and work unit. Other evidence, e.g. penetration testing documentation, may be supplied as Annexes to the SER, or as separate documents.

Example of a summary of evidence:

Evaluation of Configuration Management Capabilities (ALC_CMC.2)

CEM Work Unit	Unit Type	Type of Evidence Required
Action: ALC_CMC.2.1E – Confirm content and presentation of evidence		
ALC_CMC.2-1	Check	State that the TOE version provided for evaluation is uniquely referenced. State this reference. Provide a brief description of the referencing system used, and how this provides unique references.
ALC_CMC.2-2	Check	State that the above (ALC_CMC.1-1) reference labels (on different parts of the TOE) are consistent with each other and with the Security Target. State how the TOE provided for evaluation is labelled with its unique reference.
ALC_CMC.2-3	Examine	Describe how the procedures for identification configuration items were examined and determined that the method resulted in configuration item being labelled uniquely.

Annex D

Observation Report (OR) Format

Certification ID: XXXXXX

Observation Report (OR)			
Identification			
TOE:	(Name of TOE)	**Author:**	(Name of person writing OR)
Ref:	(CCTL Own Ref No.)	**Issue**:	(Version number)
Activity:	(Assurance Work Unit)	**Verdict:**	
Sequence No.:	(OR running number)	**Date:**	(Date of reporting)
Summary:	(Brief description of issues)		
Response Requested			
From:	(Company Name, usually the Sponsor)		
By when:	(Date)		
Deliverables Affected			
Deliverables:	(Indicate which Deliverables affected)		
Version:	(Deliverables Version Number)		
Other Deliverables Reference			
Deliverables:	(Indicate which Deliverables referenced)		
Version:	(Deliverables Version Number)		
Observation/Request			
(Describe the Observation)			
Implication			
(Describe how the issues will affect the evaluation and certification process)			
Recommended Action			
(Describe the recommended resolution to the issues raised)			

Annex E

Evaluation Technical Report (ETR) Format

Certification ID: XXXXXX

The Evaluation Technical Report (ETR) should include the following key information (further details as specified in the CC or CEM additionally apply):

1 Introduction

The Introduction covers the General Description, Scope of Evaluation and the Identifiers used in the Evaluation. In general, it provides a high-level overview of the document, including but not limiting to an executive summary of the TOE and the concepts used in the document.

2 TOE Architecture

This section describes the high-level design or architecture of TOE (ADV_ARC), summarising the major components that implement the security functions.

3 Evaluation General Information

This section presents the Evaluation Methods used and the sequence of events that have occurred in the Evaluation History. It also indicates the limitation and assumption used in the evaluation, which may influence the evaluation result.

4 Evaluation Results

This section gives a brief Introduction and a Summary of the findings and verdicts for each assurance activity. This will be based on the evaluation SERs, which report activities performed down to work unit level of Common Criteria Evaluation Methodology (CEM). Based on Common Criteria (CC) and CEM, each activity should be given a justifiable verdict. In addition, the results of testing (ATE) and vulnerability (AVA) assessment should be included in this section.

5 Conclusions and Recommendations

This section reports the Conclusions and explains the rationale of the verdicts and any Recommendations given to the Evaluation Authority, the sponsor.

6 Annexes

The Annexes include any Evaluation Evidences, Glossary, Terminology, Acronyms, SERs, ORs, OR Register and Evaluated Configuration.

Annex F

SER/ETR Review Report (RR) Format

Certification ID: XXXXXX

Report Reference	Developer's Document:
	SER/ETR:
Certifier	
Issuer	SCCS
Version & Date of RR	

Report approved	Report not approved
[X]	[ ]

If the SER/ETR is not approved:

a. A new version of the SER/ETR which addresses the anomalies detected must be delivered; and

b. The current RR shall be handled through the CCTL quality management system as a non-conformant work according to the ISO/IEC 17025. Management of the associated corrective/preventive action carried out by the CCTL will be checked during the ISO/IEC 17025 accreditation process and audit by the CSA Evaluation Authority.

Anomalies

An anomaly is a problem not detected by the evaluator. An anomaly may arise due to insufficient rationale given for the evaluation work that causes the certifier to question if the work has been carried out adequately. If the certifier does not agree with the verdict proposed by the evaluator, an anomaly may also be raised. There are only three verdicts: **Major, Minor or Recommendation**.

Types of Verdict	Description
Major	Issue must be resolved before proceeding for further evaluation
Minor	Finding that does not affect the security of the TOE. Has to be resolved before issuance of ETR.
Recommendation	A proposal for improvement

Ref.	Description	Verdict
1		
2		

Annex G

CC Alternative Reporting Procedure

Subjected to the approval by the SCCS, the CCTL may adopt the CC alternative reporting procedure with the following terms and conditions:

1. The CC alternative reporting procedure is currently in use by one of the CCRA certificate authorising scheme; and

2. At least one product had been CC certified (minimally at EAL 2) by use of the CC alternative reporting procedure; and

3. The CC alternative reporting procedure is deemed to satisfy the CC requirements.

Annex H

Task Close-Down Meeting Agenda

Certification ID: XXXXXX

The Task Close-Down Meeting or TCD is the last formal meeting between all evaluation stakeholders to close the task in a controlled manner when the SCCS has completed all evaluation activities and all stakeholders are satisfied with the Certification Report.

This is also the opportunity to review all evaluation and certification process and submit recommendations for any business processes to be improved.

The meeting should primarily cover the following:

1 CSA Evaluation Authority

a. To provide an Evaluation Summary that includes an overview of the evaluation, including technical aspects. Any evaluation issues are to be discussed.

b. To agree on the final version of the ETR and ST.

c. To agree on the sanitised version of the ST to be publicised.

d. To agree on which items of evaluation material are to be archived/ disposed of

e. To update the SCCS portal that the TOE has successfully completed evaluation.

f. To discuss the notification obligations and marketing rights conferred with the certification. This includes the usage of the CC logo.

g. To discuss and plan for future product releases, re-evaluation and/ or certificate maintenance activities.

h. Any discussion/ feedback received from the SCCS and the Sponsor/ Developer will be documented.

2 Sponsor/Developer

f. To provide feedback to the CSA Evaluation Authority on the conduct of the evaluation and the SCCS in general. This includes any operational or management processes and issues.

3 Any Other Business

To discuss any miscellaneous topics raised by any of the members.

4 Meeting wrap-up

The CSA Evaluation Authority will make closing remarks, action items, meeting summary, and review of key points/schedules, etc.

Annex I

Impact Analysis Report

<Name of TOE, Certification ID XXX>

<Date of Impact Analysis Report>

Identity of the Developer. The identity of the TOE developer is required to identify the party responsible for producing the TOE, performing the impact analysis and updating the evidence.
Configuration Control Identifiers for the Current TOE. The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the certified TOE.
Configuration Control Identifiers for the Evaluation Technical Report (ETR), Certification Report (CR), and Certified TOE. The configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.
Certified Security Target's Name, Date and Version. The developer shall report the configuration identifiers for the version of the ST related to the certified TOE.
Description of Change. The developer shall report the changes of the product. The identified changes are with regard to the product associated with the certified TOE. The developer shall report the changes to the development environment. The identified changes are with regard to the development environment of the certified TOE.
Affected Developer Evidence. For each change, the developer shall report the list of affected items of the developer evidence. For each change to the product associated with the certified TOE or to the development environment of the certified TOE, any item of the developer evidence that need to be modified in order to address the developer action elements shall be identified.
Description of Developer Evidence Modifications. The developer shall briefly describe the required modifications to the affected items of the developer evidence. For each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements shall be briefly described.
TSF Interface. Changes to the TSF Interfaces are of interest because they affect the mapping of SFRs to the interfaces. New or changed interfaces require testing to ensure they are implemented correctly. New or changed interfaces also requires design analysis

[ ] New TSF Interfaces [ ] Changed TSF interfaces [ ] No changes to TSF Interfaces	Describe:
TSF Platform (TOE Hardware). Changes to the TOE hardware may be major or minor, depending on the change. Faster equipment is not usually a concern, unless covert channels are part of the equation. New components may create new undocumented interfaces if they are accessible to untrusted users. A new operating system (OS) is more significant, again due to potentially new interfaces.	
[ ] Faster hardware [ ] New Components [ ] New OS [ ] No hardware changes	Describe:
SFRs. Changes to SFRs in the ST mean the ASE evaluation must be re-accomplished as it affects mapping consistency and the TSS. These changes also propagate throughout all the assurance evidence.	
[ ] SFR changes [ ] No SFR changes	Describe:
New Security Functions. New security functions (i.e. security functionality not covered by SFRs) provided by the product must be assessed per Scheme policy.	
[ ] New security features [ ] No new security features	Describe:
Assumptions and Objectives. Changes to assumptions and objectives may either create the need for new SFRs, or create contradictions with existing SFRs. If such changes occur, they should be examined for such effects.	
[ ] Changes to Assumptions and Objectives [ ] No changes to Assumptions and objectives	Describe:
Assurance Documents. There should be changes to assurance documents, at minimum to indicate changes to CM lists. Changes in other documents are significant and may require incremental evaluation. New interfaces or features may change guidance documents. New hardware or OSs may change installation procedures. There may also be vulnerability assessments to capture new vulnerabilities.	
[ ] ADV changes [ ] AGD changes [ ] ALC changes [ ] ATE changes [ ] AVA changes [ ] No new assurance evidence	Describe:

New Features. The product may include new non-security features. These need to be reviewed to ensure that they are categorized correctly, and that they would have no interference with the TSF	
[ ] New non-security features [ ] No new non-security features	Describe:
Bug Fixes. Updates often contain bug fixes. If these fixes were security relevant (either to security relevant software, or security vulnerabilities that were discovered in seemingly non-security-relevant software), they should be reviewed to ensure they were corrected. AVA may also require consideration for similar problems in other programs.	
[ ] Security- relevant fixes [ ] Non-security –relevant fixes [ ] No fixes	Describe:
Conclusions. For each change the developer shall report if the impact on assurance is considered minor or major. For each change the developer should provide a supporting rationale for the reported impact. In the event that the change is to the development environment, the rationale will show that there is no follow-on impact on other assurance measures.	

---------- For SCCS's use only ----------

[ ] Clear maintenance action. Only ST updates required.
[ ] Minor maintenance action. Retesting required, but nothing more.
[ ] Re-evaluation required. Reuse of evidence is possible.
[ ] Evaluation required. Evidence cannot be reused.