CCC SP-101-1

Singapore Common Criteria Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

Publication No. 1

Overview of the Scheme

June 2024
Version 8.0

FOREWORD

The Singapore Common Criteria Scheme (SCCS) is established to provide a cost effective regime for the info-communications technology (ICT) industry to evaluate and certify their IT products against the Common Criteria (CC) for Information Technology Security Evaluation (CC) standards in Singapore. These CC certifications are recognised widely through the Common Criteria Recognition Arrangement (CCRA), of which Singapore is a signatory nation.

Singapore attained the status of a Certificate Authorising Nation in January 2019 under the CCRA. The CC certificate issued under the SCCS signifies that the certified IT product is able to meet the specified security requirements operating in the specified environment.

The SCCS is owned and managed by the Evaluation Authority under the ambit of Cyber Security Agency of Singapore (CSA).

Amendment Record

Version	Date	Author	Changes
1.0 – 3.0	August 2009	Infocomm Development Authority of Singapore	Release
4.0	October 2017	Cyber Security Agency of Singapore	Alignment to CSA processes and revised CCRA.
5.0	June 2018	Cyber Security Agency of Singapore	Minor editorial revisions
6.0	January 2019	Cyber Security Agency of Singapore	Updated Singapore's status as a Certificate Authorising Nation
7.0	April 2020	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 This document provides an overview of the SCCS. It outlines the SCCS objectives, organisation and management of the SCCS, as well as providing an overview of the evaluation and certification process.

1.0.2 This document also describes the general concepts adopted in the SCCS based on CCRA and the CC. It sets out the IT security requirements and the framework for evaluation and CC certification.

2 GENERAL CONCEPTS

2.1 Common Criteria (CC)

2.1.1 The first version of CC was developed through a collaboration among national security and standards organisations in Canada, France, Germany, the Netherlands, the United Kingdom and the United States as a set of common standards to replace their respective security evaluation criteria. The CC is now recognised as the ISO/IEC 15408.

2.1.2 The CC is adopted by members of the CCRA in order to facilitate mutual recognition of evaluation and certification results. Through this, risk owners can benefit from having a wider choice of CC evaluated and certified IT products, and developers will benefit from having greater access to markets and understanding of risk owners' security requirements.

2.1.3 The CC harmonises the evaluation of IT products by defining a common set of security functions which product developers use to establish the security requirements of their IT products in a standardised language. The Common Methodology for IT Security Evaluation (CEM) is used for evaluating the product against the established security requirements, confirming that the product is able to meet these requirements with an appropriate level of assurance.

2.1.4 As a signatory nation of the CCRA, Singapore identifies with CCRA's purpose and objectives, and being a certificate consuming member, recognises certificates with claims of compliance against Common Criteria in accordance with Article 2 of the CCRA.

2.1.5 The CCRA covers certificates with claims of compliance against Common Criteria assurance components of either:

a. A collaborative Protection Profile (cPP) developed and maintained in accordance with Annex K of the Arrangement [8], with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and Flaw Remediation (ALC_FLR), developed through an International Technical Community (iTC) endorsed by the

CCRA Management Community (CCMC).

b. Evaluation Assurance Levels (EAL) 1 through 2 and ALC_FLR.

2.2 Assets and Countermeasures

2.2.1 In the context of the CC, the term “security” refers to the protection of assets. Such assets include information stored, processed and transmitted by IT products.

2.2.2 As information owners place value on their assets, threat agents also place value on these assets and seek to abuse them in a manner contrary to the interest of the owner. Examples of threat agents include hackers, malicious users, non-malicious users (causing errors unintentionally), computer processes and accidents. Threats refer to loss of confidentiality, loss of integrity and loss of availability. Threats bring risks to assets based on the likelihood of realising these threats and the resulting impact on assets.

2.2.3 Countermeasures are implemented to reduce risks to assets. Countermeasures may be IT in nature such as firewalls and smart cards, and non-IT in nature such as security guards and procedures. To reduce risks of exposing assets to the threats, owners of assets need to ascertain that the countermeasures are correct and sufficient, able to do what they claim to do and counter the threats.

2.2.4 The CC is a set of standards for specifying security requirements of IT products, evaluating whether these requirements indeed provide the identified security capabilities and evaluating whether specific IT products conform to the identified security requirements.

2.3 Security Requirements

2.3.1 Security requirements of IT products include but not limited to, confidentiality (preventing any unauthorised disclosure of information), integrity (preventing the use of or detecting any unauthorised modification of information) and availability (preventing any unauthorised withholding of information or resources).

2.3.2 In establishing the security requirements of any IT products, risk owners and developers need to consider the threats to the asset. The CC provides a catalogue of components, which the risk owners or developers can use to identify these security requirements. The hierarchical structure of these components in the CC enables risk owners and developers to find the right components to counter the threats.

2.3.3 Under the framework of the SCCS, developers can prepare and submit their security requirements for evaluation. The security requirements shall be in the form of a Security Target (ST) for a Target of Evaluation (TOE).

2.4 Target of Evaluation

2.4.1 The subject of evaluation under the SCCS is referred to as a Target of Evaluation (TOE). A TOE may be an IT product, a part of an IT product or a set of IT products.

2.4.2 There can be a difference between the TOE and the IT product that is provided for evaluation. The evaluation of a TOE which constitutes only part of an IT product, must not be misrepresented as the evaluation of the entire IT product.

2.4.3 A TOE is defined as a set of software, firmware and or hardware, and any associated guidance documentation. Guidance documentation relating to the TOE may be different from the general guidance documentation relating to the IT product. As it is usual that the IT product can be configured in many ways, the guidance documentation for a TOE is intended to set out the configurations of the TOE only.

2.5 Security Target

2.5.1 The construct for the evaluation of the countermeasures for a TOE is known as the Security Target (ST). The ST describes the assets, the threats to these assets, the countermeasures taken in the form of security objectives, and demonstrates that the countermeasures are sufficient to counter the threats.

2.5.2 Countermeasures may either be provided by the TOE or the operational environment. Evaluation under the SCCS is confined to the assessment of sufficiency and correctness of IT countermeasures provided by the TOE. Any IT or non-IT countermeasures provided by the operational environment are not assessed in the SCCS.

2.5.3 The ST expresses mechanism for realisation of the security objectives for the TOE in the form of Security Functional Requirements (SFRs). SFRs provide a set of functional components to express the security functions of IT products in a standardised way, describing the desired security behaviour (defined in CC Part 2). A TOE is deemed capable of countering threats when it meets the SFRs and the security objectives for the operational environment have been achieved.

2.5.4 The ST further expresses the activities for determining the correctness of the TOE in the form of Security Assurance Requirements (SARs). Activities include testing of TOE, examining the design representations of TOE and examining the physical security of the development environment of TOE. SARs provide a set of assurance components for expressing the assurance requirements of IT products, the evaluation activities to be performed in a standardised way (defined in CC Part 5). There is assurance in the correctness of the TOE when the SARs are met. The TOE is less likely to contain vulnerabilities that can be exploited by threat agents. The level of assurance in the correctness of the TOE is

determined by SARs, whether the SARs are “weak” or “strong”, leading to a little or a lot of assurance.

2.5.5 Detailed description of ST is given in Annex A of CC Part 1.

2.6 Protection Profile

2.6.1 A Protection Profile (PP) describes requirements for a type of TOE (e.g. firewalls) whereas an ST describes a specific TOE. A PP may be used as template for many different STs to be used in the SCCS evaluation. A PP is usually written by a user community, a group of developers or a government agency or large corporation (e.g. specifying its requirements as part of its acquisition process). Detailed description of PP is given in Annex B of CC Part 1.

2.7 Collaborative Protection Profiles (cPPs)

2.7.1 The CCRA announced in September 2012 to focus on development of collaborative Protection Profiles (cPPs) that contains the minimum set of common security functional requirements for the technology type. cPPs and associated supporting documentation are developed and maintained by International Technical Communities (iTCs) with the endorsement by all CCRA participant nations.

2.8 IT Security Evaluation and Certification

2.8.1 The SCCS provides the framework for evaluations in the areas of IT security testing, design review and implementation. Established according to the CCRA, the SCCS puts in place two levels of checks before reaching any CC certification: evaluation by an approved third-party CC Testing Laboratory (CCTL), and the evaluation results are verified by the Evaluation Authority under the ambit of CSA.

2.8.2 The Evaluation Authority establishes the requirements for approving the CCTL to operate in the SCCS according to the CCRA (refer to SCCS Publication #2). The Evaluation Authority approves the CCTL after it has been assessed for compliance with the SCCS Publication #2, and accredited by the Singapore Accreditation Council (SAC) or equivalent Accreditation Body in accordance with the ISO/IEC 17025 for testing laboratories in the specific field of IT security.

2.8.3 The Evaluation Authority provides oversight of the SAC accreditation by being represented at the SAC technical committee for assessment of testing laboratories, and supports the SAC by providing technical assessors to its CCTL assessment team. This gives confidence that the IT security evaluations carried out by the CCTL under the SCCS are performed in accordance with an accredited quality management system by independent and experience evaluators. Where necessary, the Evaluation Authority also issues additional guidance to the CCTL.

2.8.4 The SCCS Management Board is the final arbiter on all matters relating to evaluations conducted and certifications issued under the SCCS.

2.8.5 The Evaluation Authority operates within a quality management system that fulfils the requirement of the CCRA [15].

2.8.6 The SCCS certification signifies that the TOE has been assessed and found to provide or address the identified requirements. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

3 ORGANISATION AND MANAGEMENT OF SCCS

3.1 The overall policy of the SCCS is set by the Head of the Evaluation Authority. The Head of the Evaluation Authority is responsible for the direction of the SCCS, ensuring that organisation and management of the functions of evaluation and certification achieve high standards of competency, impartiality, and consistency. The Head of the Evaluation Authority approves standards, publications, and certification projects.

3.2 The Evaluation Authority provides knowledge and resources to address operational tasks to provide oversight and reporting for certification, and interacts with the international community, especially CCRA members. The Evaluation Authority approves CCTLs and monitors evaluation activities of the CCTLs, which evaluate the deliverables submitted by the developer/sponsor to the CCTL.

4 OVERVIEW OF THE CERTIFICATION SCHEME

4.1 Objectives

4.1.1 The SCCS covers TOE evaluations and certifications as described in the CC as well as assurance maintenance, to the extent that they are recognised under the CCRA. Any other CC-based evaluation will be decided by the Evaluation Authority on a case by case basis. The framework for IT security evaluation and certification is described in SCCS Publication #3.

4.1.2 In accordance with the CCRA, the objectives of the SCCS are:

a. To ensure that evaluations of IT products are performed to high and consistent standard, and are seen to contribute significantly to confidence in the security of these products;

b. To improve the availability of evaluated, security-enhanced IT products;

c. To eliminate the burden of duplicating evaluations of IT products; and

d. To continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products.

4.1.3 The SCCS is set up primarily for:

a. Developers of IT products or any other party that wishes to have an IT product evaluated (called a “sponsor”) to gain independent confirmation of the security claims of their products as specified in the relevant STs;

b. Risk owners to select suitable security products for use in their particular IT environment; and

c. Evaluators to gain independent confirmation of the results for their IT security evaluations according to the CCRA and the CC.

4.2 TOE Evaluation

a. The ST is first evaluated to determine its internal consistency, sufficiency of the claimed countermeasures provided by the TOE and its operational environment. The ST evaluation is performed using the Security Target evaluation criteria defined in the CC Part 3, according to the Security Target evaluation activity defined in the CC CEM (ASE - Assurance class for Security Target Evaluation).

b. The TOE is then evaluated for its correctness by applying requirements of assurance classes (SARs) to the TOE evaluation

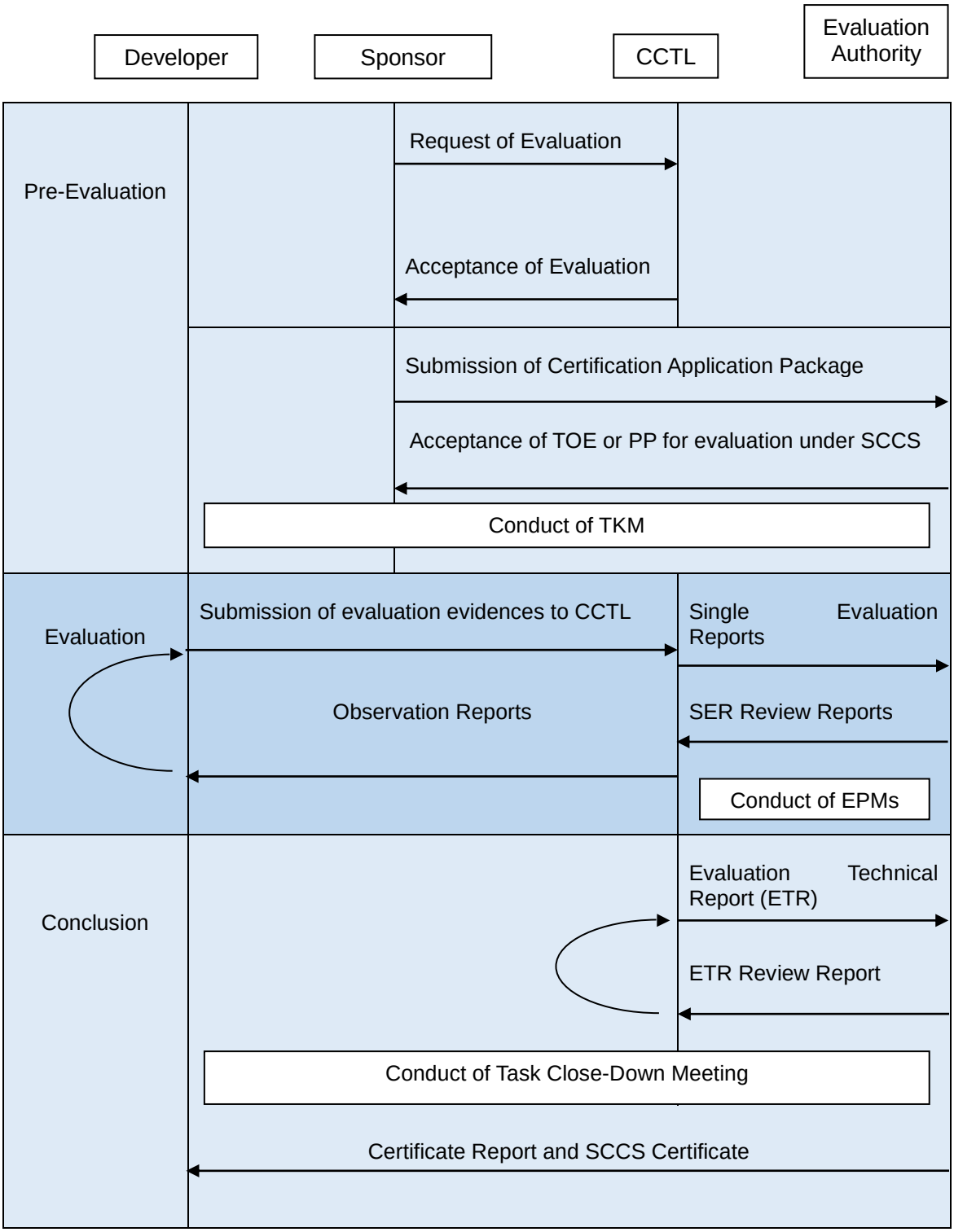
evidence, such as the TOE design documents or developer's test results (see CC Part 3 for more details). The method for applying a specific SAR corresponds with the specific evaluation activity defined in the CC CEM.

4.2.1 Evaluation Results

Reports to be generated following each evaluation activity as described in the CC CEM are listed in the SCCS Publication #3.

4.3 Typical Evaluation and Certification Process

There are three phases to the evaluation and certification process (described in detail in the SCCS Publication #3).



4.4 Cryptography

4.4.1 The CC does not address the evaluation and certification of the inherent qualities of cryptographic algorithms. CC only provides SFRs (Security Functional Requirements) for cryptographic support, in order to declare the requirements for cryptographic support, cryptographic key generation and management, and for cryptographic operation.

4.5 Criteria for Mutual Recognition

4.5.1 Recognition of the CC certificates is subject to the provisions of the CCRA. Evaluation and certification processes are carried out in a duly professional manner based on:

a. Use of accepted IT security evaluation criteria and methods that have been laid down in the CC, version of the CC endorsed by the CCRA MC;

b. Operation of an authoritative CC scheme, in another words, a national IT security evaluation and certification scheme, set up according to the CCRA requirements; and

c. CC certificates and certification reports that have been issued according to the CCRA requirements.

4.6 Mechanism for Complaints, Disputes and Appeals

4.6.1 The objective of the SCCS's Complaints, Disputes and Appeals process[1] is to track feedback from stakeholders and to ensure that issues are resolved:

a. Sponsors may contact the Evaluation Authority directly if they are dissatisfied with any services provided by the CCTL regarding their project. The Evaluation Authority holds all raised concerns in strict confidence.

b. Sponsors or CCTLs may contact the Head of the Evaluation Authority directly if they disagree with a decision made by the Evaluation Authority. The Evaluation Authority holds all raised concerns in strict confidence.

4.6.2 The Evaluation Authority shall acknowledge the receipt of a formal complaint, dispute or appeal and looks into the content of the complaint, dispute or appeal to determine whether the complaint, dispute or appeal

[1] A dispute is a written statement to the Evaluation Authority indicating disagreement with a decision made by the evaluation authority. A complaint is a written statement to the Evaluation Authority indicating dissatisfaction with a service provided by the Evaluation Authority or the CCTL. An appeal is a written statement to the Evaluation Authority indicating dissatisfaction with the resolution of a complaint or dispute.

relates to certification activities for which the Evaluation Authority is responsible.

a. If the Evaluation Authority does not accept the complaint, dispute or appeal, this is explained in writing to the party lodging the complaint.

b. If the Evaluation Authority accepts the complaint, dispute or appeal, it then processes it, recording and verifying all the necessary information (as far as possible) in order to reach a decision regarding the complaint, dispute or appeal.

4.6.3 To begin with, an attempt is made to reach an agreement regarding the disputed matter with the certifier responsible for the procedure concerned.

4.6.4 If any issue cannot be resolved to the satisfaction of the originating party, the originating party may contact the Evaluation Authority. Resolution of the issue is under the responsibility of the CSA's Senior Management Team (SMT), whose decision made on any issue raised is final.

4.7 Revocation of Certificate

4.7.1 The terms and conditions for the revocation of a certificate are given in the SCCS Publication #3.

4.8 Suspension, Withdrawal and Termination of Certification Procedure

4.8.1 The terms and conditions for the suspension, withdrawals and/or termination of certification procedure or Assurance Continuity project are given in the SCCS Publication #3.

5 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.* May 2021.

[3] Singapore Accreditation Council. *Requirements for the Application of ISO/IEC 17025, SAC-Singlas 002.* Singapore, June 2018.

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

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

[6] SCCS Publication 2 – *Requirements for Approving Common Criteria Testing Laboratory.* Version 8.0, June 2024

[7] SCCS Publication 3 – *Information Technology Security Evaluation and Certification.* Version 8.0, June 2024

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

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

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

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

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

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

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

[15] Common Criteria Recognition Arrangement Management Committee. *Operating Procedures - Conducting Shadow Certifications [Document number 2004-07-01].* 19 June 2017.

6 ACRONYMS

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

AC	Assurance Continuity
AR	Activity 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 Scheme
SFR	Security Functional Requirement
SMT	Senior Management Team
ST	Security Target
TKM	Task Kick-off Meeting
TOE	Target of Evaluation