

IC3S

CC Scheme Organization, Management and Operations

(STQC/CC/D01)

Issue : 07



CC Certification Body, STQC Directorate,
Indian Common Criteria Certification Scheme (IC3S),
MeitY, Government of India
INDIA



	Indian CC Certification Scheme	
	Issue: 07	
	Date : 25-05-2021	
		Page : 2 of 16


Table of Contents

0.1	Foreword	3
0.2	Approval and Issue.....	4
1.0	Introduction	6
1.1	Background	6
1.2	Objectives	6
1.3	Common Criteria Evaluation and Certification	7
1.4	Purpose.....	7
1.5	Scope of Certification	8
1.6	Reference	8
2.0	Scheme Overview	9
2.1	Applicant	9
2.2	Certification Body	9
2.3	Common Criteria Test Laboratory (CCTL).....	9
3.0	Process for Evaluation & Certification	10
4.0	STQC Certification Body - activities.....	11
4.1	Approval of Common Criteria Test Laboratory (CCTL)	12
4.2	Evaluation Technical Oversight.....	12
4.3	Technical oversight of assurance continuity activities	13
4.4	Website Maintenance	14
4.5	Quality Management	14
4.6	CC Certificates	14
4.8	Recertification	15
	Annexure I - Flow Diagram of the process for CC Certification.....	16

 गुणोत्कर्षं समृद्धिः	Indian CC Certification Scheme	
		Issue: 07
		Date : 25-05-2021
		Page : 3 of 16

0.1 Foreword

This document describes the Indian Common Criteria Certification Scheme (IC3S). It fulfills one of the key requirements of the Arrangement on the Recognition of Common Criteria Certificates (CCRA) in the field of Information Technology Security. Ministry of Electronics and Information Technology (MeitY), STQC Directorate is one of the signatories of that arrangement.

 गुणोत्कर्षं समृद्धिः	Indian CC Certification Scheme	
		Issue: 07
		Date : 25-05-2021
		Page : 4 of 16

0.2 Approval and Issue


This document is the property of Indian Common Criteria Certification Scheme (IC3S) and should not be reproduced in part or full without the written consent.

Reviewed by : Management Representative

Approved by : Head, IC3S Scheme

Note:

- Management Representative is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

	Indian CC Certification Scheme	
	Issue : 07	
	Date : 25-05-2021	
		Page : 6 of 16

1.0 Introduction

1.1 Background

The Indian Common Criteria Certification Scheme (IC3S) provides for the security evaluations of the IT Products to the Common Criteria (CC) standard by approved evaluation laboratories.

Evaluation technical oversight and certification of the results is performed by a Certification Body (CB) within the Government of India and is operated by the Standardization Testing and Quality Certification Directorate (STQC Directorate)(<http://www.Commoncriteria-India.gov.in>).


There are two types of security requirements that are evaluated under the Scheme i.e. security functional requirements and assurance requirements. The Functional requirements describe the desired security services to be provided by an IT product and Assurance requirements describe the requirements for evaluation analysis and testing. The Assurance requirements are expressed in the form of Evaluation Assurance Levels (EAL), a set of 7 hierarchical levels defined within the CC standard. CC evaluations that are certified in India (up to EAL4) shall be recognized by member of countries that are signatories to the Arrangement on the Recognition of Common Criteria Certificates (CCRA) after successful CCRA audit.

1.2 Objectives

Ministry of Electronics & Information Technology, STQC Directorate have the following objectives in developing, operating & maintaining Common Criteria based IT Security Evaluation & Certification Scheme:

- a) To meet the needs of government and industry for cost-effective evaluation of IT products;
- b) To encourage the formation of commercial security testing laboratories
- c) To ensure that security evaluations of IT products are performed to consistent standards;
- d) To improve the availability of evaluated IT products.

The scheme is intended to serve many communities of interest with very diverse roles and responsibilities. This community includes IT product

	Indian CC Certification Scheme	
	Issue: 07	
	Date : 25-05-2021	
		Page : 7 of 16

developers, product vendors, acquisition/procurement authorities, consumers of IT products etc. Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

1.3 Common Criteria Evaluation and Certification


Common Criteria Evaluation and Certification is an impartial assessment of an IT product by an independent body. This provides users of such products with the confidence in the security functionality and assurance provided. The IT products to be evaluated are referred to as the Target of Evaluation (TOE). Certification provides independent confirmation of the validity of evaluation results, and thereby ensures comparability of these results across all evaluations under the scheme and facilitates mutual recognition of results between national schemes. Certification confirms that the TOE meets its security target to the claimed assurance level and that the evaluation has been conducted in accordance with the Standard of the scheme.

The certification does not endorse a TOE in any other respect. Moreover, it is not a guarantee that the TOE is completely free of exploitable vulnerabilities. There will remain a small probability that some exploitable vulnerability remains undiscovered whereas the probability of this decreases as the assurance level increases. The certification applies to a specific version of a TOE. However, the scheme provides opportunities by which the certification status of a TOE can be maintained without always requiring a full re-evaluation on every change of version of TOE.

1.4 Purpose

The participation in the scheme and its associated evaluation & certification activities is strictly voluntary (unless mandated by government policy or regulations). In addition, organizations may undertake alternative activities to use Common Criteria and to demonstrate product conformance to IT security requirements.

The purpose of this document is to provide an overview of the scheme, to briefly explain what comprises a CC evaluation, and to provide details on the various aspects of Certification body (CB) operations, referencing other documents where appropriate.

	Indian CC Certification Scheme	
	Issue: 07	
	Date : 25-05-2021	
		Page : 8 of 16

1.5 Scope of Certification

Present scope of CC Certification covers Boundary Protection Devices, Network & Network related devices & systems and Operating Systems as per CC standard up to EAL 4.

1.6 Reference


[CC] Common Criteria for Information Technology Security Evaluation: is the IT security evaluation criteria

[CEM] Common Methodology for Information Technology Security Evaluation: is the IT security evaluation methodology used by the IC3S;

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the field of

Information Technology Security: is the arrangement between its signatories for the recognition of evaluations performed by any of the signatories.

*(Please refer **Master List of Documents** for latest version of the documents)*

	Indian CC Certification Scheme	
	Issue : 07	
	Date : 25-05-2021	
		Page : 9 of 16

2.0 Scheme Overview

The IT security evaluation & certification Scheme based on Common Criteria standards, herein after referred as the Indian Common Criteria Certification Scheme (IC3S) is established by Govt. of India under Ministry of Electronics and Information Technology (MeitY), STQC Directorate to evaluate & certify the security features in Information Technology (IT) products and systems. It also provides a framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

- a) Applicant (Sponsor/Developer) of IT security evaluations
- b) STQC Certification Body
- c) Common Criteria Testing Laboratories (CCTLs).

2.1 Applicant


In the context of the Common Criteria Scheme, an Applicant is the party requesting and paying for the security evaluation and certification of an IT product or Protection profile. The Applicant is often the product or profile developer, but could also be a government agency, industry consortium, or other organization seeking to obtain an IT security certification.

2.2 Certification Body

The Certification Body is managed by STQC Directorate. The Certification Body approves participation of security testing laboratories in the scheme in accordance with its established policies and procedures. It also provides technical guidance to those testing laboratories validates the results of IT security evaluations for conformance to the Common Criteria standards and serves as an interface to other nations on the recognition of such evaluations. An overview of operations of the Certification Body is defined in the document STQC/CC/D02-“Quality Manual”.

2.3 Common Criteria Test Laboratory (CCTL)

IT security evaluations are conducted by testing laboratories accredited and approved by Certification Body. These approved testing laboratories are called Common Criteria Testing Laboratories (CCTL). The purpose of the

	Indian CC Certification Scheme	
	Issue : 07	
	Date : 25-05-2021	
		Page : 10 of 16


accreditation is to ensure that laboratories meet the requirements of ISO/IEC 17025 (General Requirements for the Competence of Calibration and Testing Laboratories) and the scheme specific requirements for IT security evaluations. The applicant laboratories are audited by CB to verify compliance to the requirements. In case, the applicant laboratory is already accredited by any agency in India or abroad as per the requirements of ISO/IEC 17025, CB may consider to exempt relevant requirements in its audit process.

The details of requirements are provided in the document, STQC/CC/D04-“Requirements for Test Laboratories”.

3.0 Process for Evaluation & Certification

There are two types of CC evaluations that are performed under the Scheme: PP evaluations and IT product evaluations. PP evaluation requires evaluating whether a set of IT security requirements is appropriate, given the security environment that is being targeted. An IT product evaluation is with reference to a Security Target (ST), which describes the security requirements that are to be met by the IT product.

An applicant interested in CC certification of IT product or protection profile is required to approach CB with its security target. The Certification Body (CB) formally accepts the application. CB appoints a validator and assign evaluation activity to CCTL. It is communicated to the applicant organisation. The CCTL, in consultation with CB, finalizes an evaluation work plan with the Applicant. The CCTL conducts the evaluation according to the requirements of the Common Evaluation Methodology (CEM) for Information Technology Security Evaluation which describes how evaluation activities are to be performed. The CB performs technical oversight of these evaluations, and identifies any concerns, requiring corrective action by the CCTL. At the conclusion of the CC evaluation, the CCTL provides an Evaluation Technical Report (ETR) to the CB. The ETR is a proprietary document that describes the details of all evaluation activities that were performed and is not released to the public. The Validator appointed by the Certification Body is continuously associated with evaluation project in CCTL, reviews all evaluation work outputs like worksheets, observation report, ETR etc. on behalf of Certification Body. A process flow for IT Security evaluation & certification is presented in **Annexure I**.

	Indian CC Certification Scheme	
	Issue: 07	
	Date : 25-05-2021	
		Page : 11 of 16


The scheme requires all documents to be in English language.

4.0 STQC Certification Body - activities

The principal objective of the STQC Certification Body is to ensure the provision of competent IT security evaluation and certification services for both government and industry. The Certification Body has the ultimate responsibility for the operation of the scheme in accordance with its policies and procedures as per the requirements of ISO/IEC 17065 (Conformity Assessment- Requirements for bodies certifying products, processes and services) and CCRA annexure B & C. STQC Directorate is responsible for providing sufficient resources to the Certification Body so that it may carry out its responsibilities. The STQC Certification Body must ensure that appropriate mechanisms are in place to protect the interests of all parties within the scheme participating in the process of IT security evaluation. Any dispute brought forth by a participating party, (i.e., Applicant of an evaluation, product or protection profile developer, or CCTL), concerning the operation of the scheme or any of its associated activities shall be referred to the Certification Body for resolution. In disputes involving the Certification Body, may be referred to the Chairman, Certification Body under the provision of the document, STQC/CC/P07- “Appeal Procedure”.

Decisions to resolve high-level disagreements amongst the stakeholders shall also be captured and made available to CCTLs/validators/certification team personnel under the scheme through mail at least once in 6 months or as and when required.

The CB has several responsibilities, including approval of CCTL to operate under the Scheme, performing evaluation technical oversight, generating CC certificates and associated reports, and maintaining a scheme website where certification results are posted for all scheme evaluations. The CB also has the responsibility to see that procedures are in place within the scheme to ensure that the sensitive information relating to products and protection profiles under evaluation and to the process of evaluation itself is appropriately handled and given the security protection it requires and that those procedures are routinely followed. Further details are provided within this chapter, for each of these CB activities.

	Indian CC Certification Scheme	
	Issue : 07	
	Date : 25-05-2021	
		Page : 12 of 16

4.1 Approval of Common Criteria Test Laboratory (CCTL)

CCTLs are testing laboratories that are accredited by the CB and listed on an approved laboratories list by the STQC Certification Body. These laboratories must meet the requirements of:

- a) **ISO/IEC 17025** -General Requirements for the Competence of Testing and Calibration Laboratories.
- b) Specific criteria for IT security evaluations and other requirements of the scheme as defined by the STQC Certification Body in the document STQC/CC/D03-“Accreditation Process for Enlistment and Operation of Labs under IC3S”.


CCTLs enter into contractual agreements with Applicants to conduct security evaluations of IT products and protection profiles using STQC-approved test methods derived from the Common Criteria, Common Evaluation Methodology and other technology-based sources. The IT security evaluations are carried out in accordance with the policies and procedures of the scheme. The CCTL also has to demonstrate to the satisfaction of the CB that it is technically competent in the specific field of IT security evaluation and that it is in a position to comply in full with the rules of the Scheme concerned

4.2 Evaluation Technical Oversight

CC evaluations of IT products (also referred to as the Target of Evaluation, or TOE) are conducted in two phases. The first phase is an evaluation of the ST, and the second is an evaluation of the IT product's conformance against the security requirements expressed in the ST. The CB conducts evaluation oversight activities on an ongoing basis and raises observation reports in response to identified concerns. These evaluation oversight activities comprise the following:

- Independently performing a subset of the evaluation work, and comparing the results with that of the CCTL;
- Directly observing evaluation activities in progress; and
- Reviewing evaluation reports generated by the CCTL.

For additional information refer to the scheme Document, STQC/CC/D08 – “Technical Oversight for TOE Evaluation”.

	Indian CC Certification Scheme	
	Issue: 07	
	Date : 25-05-2021	
		Page : 13 of 16

CC evaluations of Protection Profiles (PP) require CB to still conduct technical oversight of the CCTL evaluation work in order to ensure quality, raising observation reports where concerns are identified. Given the limited scope of PP evaluation activities, it is not applicable for the CB to directly observe evaluation activities in progress. As a result, the CB's evaluation oversight activities comprise the following:

- Independently performing a subset of the evaluation work, and comparing the results with that of the CCTL
- Directly observing evaluation activities in progress; and
- Reviewing evaluation reports generated by the CCTL.

For additional information refer to the scheme document, *STQC/CC/D09–“Technical Oversight for PP Evaluation”*.


Technical oversight begins with the acceptance of an IT security evaluation into the scheme by the STQC Certification Body. During the evaluation, the validators appointed by the Certification Body routinely interacts with the CCTL and the Applicant of the evaluation by:

- a) Providing information in technical and non-technical areas deemed essential to the success of the IT security evaluation;
- b) Requiring and receiving information in technical and non-technical areas deemed essential to the certification process;
- c) Working together to resolve important technical issues.

The Certification Body will issue strict guidelines on how these technical overview activities will be implemented within the scheme in order to establish the appropriate level of expectation on behalf of Applicants and CCTLs. The specific details of the technical overview process and activities associated with that process are described in Scheme documents, *STQC/CC/D08–“Technical oversight for TOE evaluation”* and *STQC/CC/D09 – “Technical oversight for PP evaluation”*.

4.3 Technical oversight of assurance continuity activities

Assurance continuity is the process by which changes to a previously-certified IT Product is assessed, to determine whether the assurance can be maintained through an impact assessment of the changes, rather than going through a costly re-evaluation to the CC.

	Indian CC Certification Scheme	
	Issue: 07	
	Date : 25-05-2021	
		Page : 14 of 16

The CB performs technical oversight of assurance continuity requests in the following manner:

- Assessing the nature of the changes to the IT product, and determining whether the changes are sufficiently minor that assurance maintenance is an appropriate option; and
- Reviewing in detail the Impact Analysis Report (IAR) that is provided by the Developer, to determine whether the analysis of the changes is complete, correct, and sufficiently rigorous.

Additional information on the technical oversight of assurance continuity activities can be found in Scheme document, STQC/CC/D10- “*Technical oversight for Assurance Continuity*”.

4.4 Website Maintenance

The CB maintains a public website that contains a broad range of information about the Scheme including, but not limited to: CC documentation; Scheme process documentation; certification results for CC evaluations; assurance maintenance results; and contact information for CCTL. The CB conducts regular reviews of the Scheme website to ensure that the information is correct and up to date. The certified product listed on the website will be moved to archive section after completion of five years.


4.5 Quality Management

The CB has put in place a quality system to ensure that all CB activities continue to be performed to a high degree of quality in line with the requirements of ISO/IEC 17065 and CCRA Annexure B & C. Detailed procedures have been developed that cover all aspects of CB operations, and a quality audit is performed on an annual basis.

Additional information on how quality is maintained within the CB can be found in the document, STQC/CC/D02- “Quality Manual”.

4.6 CC Certificates

At the successful completion of a CC evaluation, the CB generates a CC certificate, and prepares a Certification Report (CR), that describes the results of the evaluation. The CR is based on a draft that is provided by the

	Indian CC Certification Scheme	
		Issue: 07
		Date : 25-05-2021
		Page : 15 of 16

CCTL, and all CRs created within this comply with the content requirements mandated in Annex B & C of the CCRA.

Once the Certification Body has approved the final certification report, a Common Criteria certificate will be issued. STQC Certification Body is the certificate-issuing authorities for the scheme. The Head, CC Scheme, will sign the certificate, indicating acceptance of the points articulated above. After the certificate has been issued to the Applicant organization of the security evaluation, an appropriate entry will be made on the STQC Certified Products List. The certificate applies only to the specific version and release of the IT product in its evaluated configuration or the particular version of the protection profile as evaluated. A Feedback form (STQC/CC/F28) will be sent with Certificate to applicant. An Applicant of an evaluation shall only market an IT product or a Protection Profile as an evaluated product or an evaluated profile, respectively, on the basis of the certification report and accompanying Common Criteria certificate published by the Certification Body. The issuance of a certificate does not imply endorsement of an IT product or protection profile by STQC or any other agency of the Indian Government. Details on Common Criteria Certificates can be found in the document, STQC/CC/D05 – “Certificate”.

4.7 Timeline for CC Certification


Timeline for CC evaluation/Certification depends on Evaluation Assurance Level. Tentative timeline for each level is given below.

Level 1	:	6 months
Level 2	:	8 months
Level 3	:	12 Months
Level 4	:	14 months

(subject to bi-annual review to avoid any unreasonable delay)

4.8 Recertification

The organization if interested needs to apply afresh for recertification after the completion of validity period of 5 years.

	Indian CC Certification Scheme	
	Issue : 07	
	Date : 25-05-2021	
		Page : 16 of 16

Annexure I - Flow Diagram of the process for CC Certification

