IC3S

Guidance to Applicants

(STQC/CC/D06)

Issue :06

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

Table of Contents

0.1 APPROVAL AND ISSUE 3

0.2 AMENDMENT RECORD 4

1.0 INTRODUCTION 5

1.1 COMMON CRITERIA 5

2.0 THE INDIAN COMMON CRITERIA CERTIFICATION SCHEME (IC3S) 6

2.1 EVALUATION PROCESS AND INDIAN COMMON CRITERIA CERTIFICATION SCHEME (IC3S) 6

2.1.1 Steps for applying for CC Certification 6

2.2 DETAILS OF THE STEPS 7

2.2.1 Contacting IC3S and submission of formal application 7

2.2.2 Assessment Process 7

2.2.3 Flow Diagram of the process for CC Certification 9

2.2.4 CC documentations 10

3.0 ANNEXURE I 11

A. DEVELOPER'S EVALUATION EVIDENCES REQUIRED TO BE SUBMITTED FOR EAL 1 CC EVALUATION: 11

B. DEVELOPER'S EVALUATION EVIDENCES REQUIRED TO BE SUBMITTED FOR EAL 2 CC EVALUATIONS: 11

C. DEVELOPER'S EVALUATION EVIDENCES REQUIRED TO BE SUBMITTED FOR EAL 3 CC EVALUATIONS: 12

D. DEVELOPER'S EVALUATION EVIDENCES REQUIRED TO BE SUBMITTED FOR EAL 4 CC EVALUATIONS: 12

0.1 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, CC 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.

0.2 Amendment Record

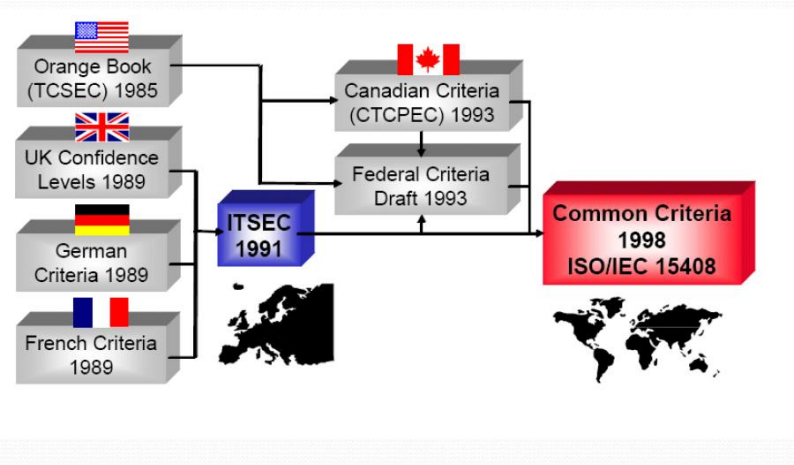
Sl. No.	Date	Issue	Reason of Change /Change Details
1.	01-12-11	01	First Issue
2.	16-10-12	02	Comprehensive review of CC Scheme documentation
3.	02-05-13	03	Incorporation of recommendations of the CCRA Shadow audit team. The flow diagram in section 2.2.2 has been modified to include cursory evaluation of ST received with application.
4.	25-05-18	04	Comprehensive review of CC Scheme documentation
5.	14-06-19	05	Change in Contact details
6.	29.05.20	06	Contact details removed

1.0 Introduction

1.1 Common Criteria

Common Criteria provides a framework for users to specify their security functional and assurance requirements, vendors to implement and/or make claims about the security attributes of their products, and testing laboratories for evaluating the products to determine if they actually meet the claims.

- Common Criteria provides assurance that the process of specification, implementation and evaluation of anIT security product has been conducted in a rigorous and standard manner
- The Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the International Community.



2.0 The Indian Common Criteria Certification Scheme (IC3S)

Ministry of Electronics & Information Technology is the nodal agency for all activities related to policy and promotion of IT, internet and E-Commerce. STQC Directorate, as a part of the Ministry, is mandated to align itself w.r.t. the objectives of Ministry and provide support and services to the users in line with these objectives. Over the years STQC's Core Competence has been around Standardisation, Test & Calibration and Certification.With the Indian IT Act 2008 coming into existence, Ministry has taken up several initiatives to facilitate the spread the use of IT and promotion of E-Commerce. Owing to its Core Competence, STQC is providing IT related services concerning Standardisation, Test & Certification. The "Common Criteria Certification" is one such focused effort on certification.

The main beneficiariesof this programme are Developer of IT Products or Protection profiles, Sponsors, Common Criteria Test Laboratory (CCTL) and Certification Body. The scheme also provides a framework for the International Mutual Recognition of such certificates with the other member countries of CCRA (Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology).The Certification Body is the STQC Directorate, Ministry of Electronics and Information Technology (MeitY), Govt. of India.

This document prescribes the guidelines to the applicant for applying for CC Certification of the product.

2.1 Evaluation process and Indian common criteria certification scheme(IC3S)

2.1.1 Steps for applying for CC Certification

The process for evaluation of IT security products consist of the following steps:

a) Contacting IC3S (by prospective Developer / Sponsor)
b) Submission of formal application along with the application fee
c) Submission of Documentation along with the application.
d) Developer / Sponsor Contacting CCTL for Evaluation.
e) Evaluation and Validation
f) Grant of Certification

2.2 Details of the steps

2.2.1 Contacting IC3S and submission of formal application

A Developer / Sponsor shall contact Head, CC Scheme for product certification along with preliminary information like identification of the Type of product, TOE, ST, Complying PP, contact person, area of technology of IT security product (for which evaluation will be carried out) and target EAL.

On receipt of such communication, IC3S will instruct the potential applicant for making formal application to designated point of contact of IC3S or may guide them to choose right EAL.

The formal application must be signed by the competent authority (documentary evidence in respect of authority is required to be submitted along with the application). The application shall also be accompanied with necessary nonrefundable registration fees.

2.2.2 Assessment Process

a) The formal application made by the Developer / Sponsor along with "Security Target" shall be treated as first official record of the certification under CC. The information received through formal application should be used to assess the identification of TOE and PP Claimed.

b) The application shall be assessed by CB to check the completeness and correctness.

c) CB shall assign a CCTL for evaluation of the product with information to sponsor/Developer.

d) CCTL shall communicate to the Developer / Sponsor the work evaluation plan.

e) Contract shall be signed between the Developer/ Sponsor and the CCTL.

f) Evaluation and Certification Services: The evaluation and certification projects shall only be made available through IC3S. In case the developer/sponsor contacts the CCTL in this regard, CCTL shall direct them to IC3S. The first meeting may be needed between Certification body, the developer/sponsor and the CCTL to understand the TOE and target EAL.

g) Supply of Documentation to the CCTL by Developer: All documentation supplied to CCTL must be in encrypted softcopy format, either on suitable removable media or through secure repository or through secure email.

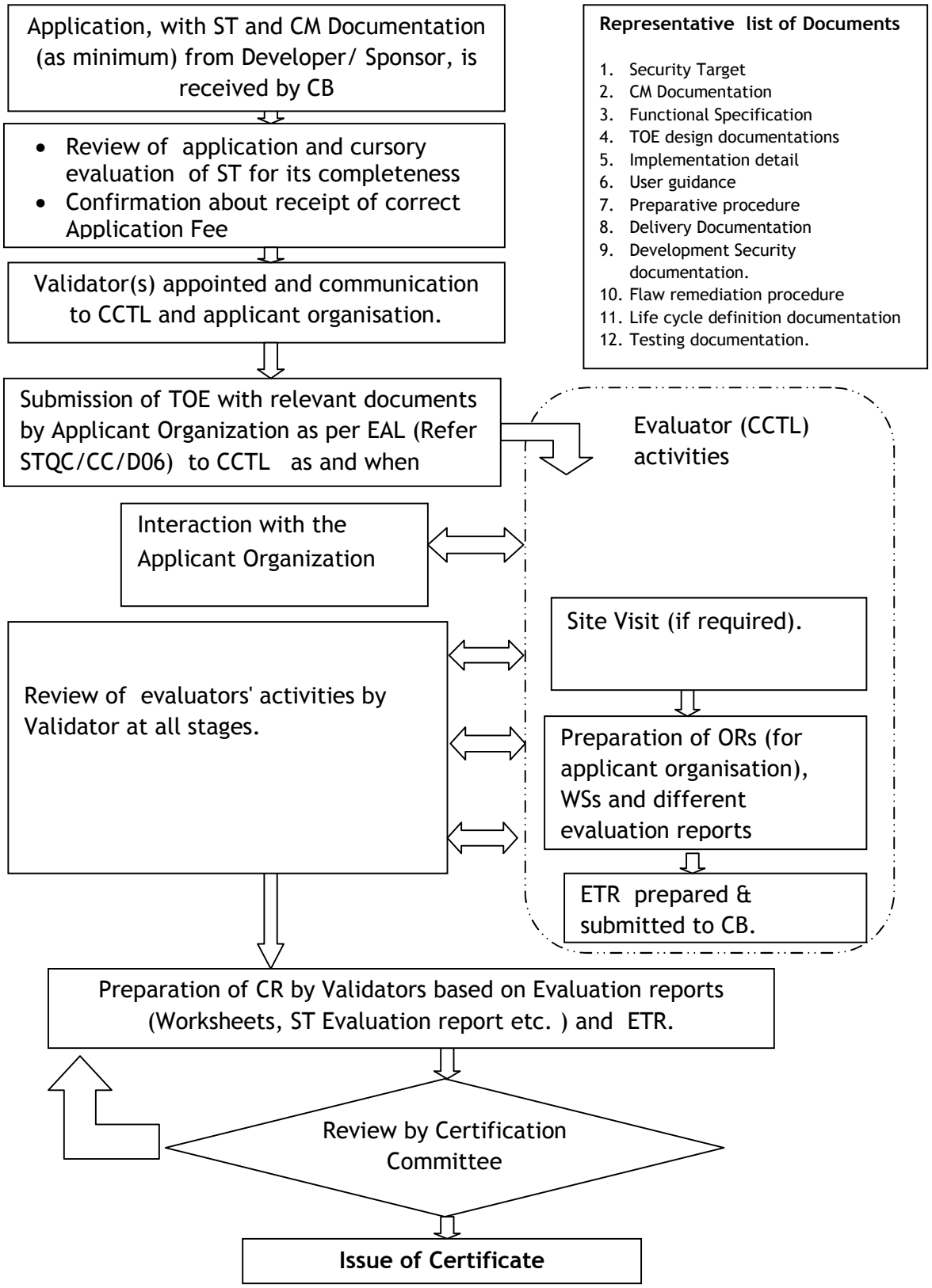
h) Security Target Review: CCTL shall carry out the formal evaluation of the Security Target according to the appropriate criteria and methodology, and ensure that the Security Target defines a TOE which corresponds to the scope of evaluation agreed.

i) Evaluation shall be done by CCTL.

j) The validator examines the Evaluation report to determine that the information content and structure requirements have been satisfied. Once the validator is satisfied with the content of the ETR, the validator then generates a draft CR.

k) The CR is presented to the Certification Committee. The Head of the Certification Body is the final authority concerning the content of the certificate of evaluation and the associated CR.

2.2.3 Flow Diagram of the process for CC Certification



2.2.4 CC documentations

CC Documentation required are :

- Security Target
- Configuration Management documentation
- Functionality Specification
- TOE design documentation
- Implementation details
- User guidance
- Preparative procedure
- Delivery documentation
- Development security documentation
- Flaw remediation procedures
- Life cycle definition documentation
- Testing documentation

3.0 Annexure I

Documents required for EAL 1, EAL2, EAL3, EAL4 CC Evaluation

A. Developer's evaluation evidences required to be submitted for EAL 1 CC evaluation:

1. Security Target (ASE) Evaluation
2. Development (ADV)
   - 2.1 Functional Specification (ADV_FSP.1)
3. Guidance (AGD)
   - 3.1 Preparative Procedures (AGD_PRE.1)
   - 3.2 Operational Procedures (AGD_OPE.1)
4. Life-cycle Support (ALC)
   - 3.1 Configuration Management (ALC_CMC.1 and ALC_CMS.1)

B. Developer's evaluation evidences required to be submitted for EAL 2 CC evaluations:

1. Security Target (ASE) Evaluation
2. Development (ADV)
   - 2.1 Functional Specification (ADV_FSP.2)
   - 2.2 Design document (ADV_TDS.1)
   - 2.3 Security architecture (ADV_ARC.1)
3. Guidance (AGD)
   - 3.1 Preparative Procedure (AGD_PRE.1)
   - 3.2 Operational Procedure (AGD_OPE.1)
4. Life-cycle Support (ALC)
   - 4.1 Configuration Management (ALC_CMC.2 and ALC_CMS.2)
   - 4.2 Delivery procedure (ALC_DEL..1)
5. Tests (ATE)
   - 5.1 Functional test (ATE_FUN.1)
   - 5.2 Test coverage (ATE_COV.1)

C. Developer's evaluation evidences required to be submitted for EAL 3 CC evaluations:

1. Security Target (ASE) Evaluation
2. Developments (ADV)
   - 2.1 Functional Specification (ADV_FSP.3)
   - 2.2 Design document (ADV_TDS.2)
   - 2.3 Security architecture (ADV_ARC.1)
3. Guidance (AGD)
   - 3.1 Preparative Procedure (AGD_PRE.1)
   - 3.2 Operational Procedure (AGD_OPE.1)
4. Life-cycle Support(ALC)
   - 4.1 Configuration Management (ALC_CMC.3 and ALC_CMS.3)
   - 4.2 Delivery procedure (ALC_DEL.1)
   - 4.3 Development Security (ALC_DVS.1)
   - 4.4 Life Cycle Definition(ALC_LCD.1)
5. Tests (ATE)
   - 5.1 Functional test (ATE_FUN.1)
   - 5.2 Test coverage (ATE_COV.2)
   - 5.3 Depth Analysis (ATE_DPT.1)

D. Developer's evaluation evidences required to be submitted for EAL 4 CC evaluations:

1. Security Target (ASE) Evaluation
2. Developments (ADV)
   - 2.1 Functional Specification (ADV_FSP.4)
   - 2.2 Design document (ADV_TDS.3)
   - 2.3 Security architecture (ADV_ARC.1)
   - 2.4 Implementation Representation ((ADV_IMP.1)
3. Guidance (AGD)
   - 3.1 Preparative Procedure (AGD_PRE.1)
   - 3.2 Operational Procedure (AGD_OPE.1)

4. **Life-cycle Support (ALC)**
   - 4.1 **Configuration Management (ALC_CMC.4 and ALC_CMS.4)**
   - 4.2 **Delivery procedure (ALC_DEL.1)**
   - 4.3 **Development Security(ALC_DVS.1)**
   - 4.4 **Life Cycle definition (ALC_LCD.1)**
   - 4.5 **Tools and techniques (ALC_TAT.1)**
5. **Tests (ATE)**
   - 5.1 **Functional test (ATE_FUN.1)**
   - 5.2 **Test coverage (ATE_COV.2)**
   - 5.3 **Depth Analysis (ATE_DPT.1)**