IC3S

Guidance on Evaluation of Cryptographic Security Mechanism of TOE

(STQC/CC/D16)

Issue : 03

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

Table of Contents

0.1 Approval and Issue

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.

0.1 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.	25-05-18	03	Comprehensive review of CC Scheme documentation

1.0 Introduction

Cryptography is considered as most effective mechanism to protect Confidentiality, Integrity and Availability of information and used commonly available as one of the Security Functional requirements (SFR) in TOE.

Traditionally the encryption mechanisms are of two types, 'symmetric key' or 'private key' and 'asymmetric key' or 'public key'; however, use of a combination of both (hybrid) are also quite popular.

The present CC standard has kept evaluation of the strength of cryptographicsecurity algorithm out of their scope and left to the individual country specific CC scheme to adopt suitable methodology [A.5 CEM].However, the verification of correct functionality of the cryptographic mechanism needs to be carried out by the CCTL during evaluation.

2.0 Approach of IC3S

The scheme is primarily aimed for software IT security products and the target evaluation level is up to EAL 4. The following approach shall be followed :

a) For evaluation at level below EAL 4, the TOE must use the standard cryptographic algorithms (like PKCS #1 for RSA, FIPS 197 for AES etc.) and the developer must provide the test report using the standard test vectors published by NIST, U.S. The CCTL shall verify the correctness of implementation of the cryptographic mechanism by re testing using the standard test vectors again.

b) For evaluation at EAL 4, the TOE shall use not only the standards cryptographic algorithm (like PKCS #1 for RSA, FIPS 197 for AES etc) but also the same shall be used at least in FIPS 140-2 Level 1 mode in the TOE. The developer shall provide enough evidence in support of this along with the test report using standard test vectors.

c) However, if the adopted PP specifies the requirement of testing and evaluation of the cryptographic mechanism explicitly, the same shall be followed.