Developing Common Criteria Compliant Security Products

Subhendu Das¹, Tapas Bandyopadhyay² and Malabika Ghose³
¹Scientist F, STQC IT Services, Kolkata,
²Scientist E, STQC IT Services, Kolkata,
³Scientist E, STQC IT Services, Kolkata,
¹subhendu@ertleast.org, ²tapas@ertleast.org and ³malabika@ertleast.org

ABSTRACT
With the rise of information security breaches and the running of technology at its high gear on the information superhighway, protection of confidential and vital information never has been so crucial. In addition, with the IT security services offered by the IT security products, the needs have been felt to have some kind of assurance to these services[4]. The IT security products are used to counter the security threats to the critical assets. The selection and application of IT security products are integral part of a mission critical IT infrastructure. The Common Criteria (CC) was developed to facilitate common understanding among the stakeholders and consistent evaluations of IT security products [1, 2]. It is an international effort to define common set of IT Security requirements and their evaluation methodology in such a way that would receive mutual recognition among users, customers and vendors across the participating countries. The security functions are implemented in the Target of Evaluation (TOE) to achieve specific security objectives, aimed to mitigate IT security threats and capable to adhere organizational security policies, if necessary. The Common Criteria certification process not only include the testing of the security functions of the product and its vulnerability assessment but also include evaluation of product documentations (like security specification, design document and implementation representation of the TOE) and evaluation of development processes (like Configuration management, Secure Development and delivery etc)[3]. The level of confidence drawn from the evaluation process are presently described as EAL 1 to 7 which varies with increasing depth of inspection and obviously with the increasing volume of evaluation evidences. Developers wishing to develop CC compliant IT security product need to define target level of EAL at the beginning of the development process. They need to produce various products and process related documents throughout the life-cycle to provide inputs to the evaluation body. The depth of these documents varies with the targeted EAL. These evaluation evidence documents usually go through several iterations to fulfill the requirements of CC standard. These documents produced by the developer give confidence to the evaluators that the features implemented in the TOE are an accurate reflection of the security functionalities as defined in the security target document (ST).

This paper aims to direct the developers of the IT security products in respect of the requirements of CC which will enable them to produce CC compliant evaluation evidences which in turn produce CC compliant products.

KEYWORDS
Common criteria (CC), Security Target (ST), Target of Evaluation (TOE), Evaluation evidences, Functional specification (FSP), Evaluation assurance level (EAL), configuration management (CM),Life cycle definition (LCD), Development security (DVS)

1. INTRODUCTION
In todays increasingly online IT enabled environment, security is of keen concern to all user groups. Information security is an ever-evolving challenge, requiring proper attention and due care to have a secure and sustainable system for continued business operation. Information security is usually achieved through implementation of some technology solutions like firewall, Access control devices, smart cards etc., offering security services within a defined Management framework of Information Security. While implementing systems and software solutions, organization needs to have confidence in the features of the IT security products. The Common Criteria (CC) is designed to provide an impartial assessment of the security characteristics of IT products by an independent entity [2]. Once an IT security product is CC certified, then the users will able to judge the product in a common framework of security definition and assessment. This will not only help them to determine whether particular product meets the intended security requirements but also help to judge the relative security of competing IT products [4].

The trust and confidence necessary on the security functions offered by the product is very much dependent of the security environment of the device and the asset to be protected [3]. Common Criteria has provisioned different Evaluation Assurance Levels (EAL) to address these requirements. Hence, two products may offer same security services but may be evaluated at different EAL to commensurate with the requirement of the use. A product certified at higher EAL does not necessarily mean that it offers more security than the one evaluated at lower EAL unless the same security features are not included. The difference lies in trust and confidence or
assurance from the product. As higher EAL means higher assurance from the product, the depth of inspection increases and so the efforts as we move from lower EAL to higher. Common Criteria standards though described the security functional and assurance components for EAL 1 to 7 but limit its published evaluation methodology up to EAL 4 [3]. The products used in non-military application are usually evaluated up to EAL 4.

2. SYSTEM DEVELOPMENT LIFE CYCLE (SDLC):
The product developers usually adopt a system or software development life cycle (SDLC) methodologies to control the development activities of products. Generally, the SDLC process involves the different phases like Requirement Analysis, Design, Product realization, Testing maintenance etc. The general model for SDLC is depicted in fig 1.

![SDLC Diagram](image)

Fig 1: System /software development life cycle (SDLC)

2.1 REQUIREMENT ANALYSIS
In this stage, the information about the product features, purpose, user profiles, application environment, required interfaces etc are captured. The input of this stage is the high-level requirements that the product is supposed to offer. The product features are refined into a set of requirements. These requirements define the major functions of the intended product.

The requirement analysis usually extended till end of development life cycle as it gets refined through several iteration based on the inputs from subsequent stages like Design, Product Realization and testing. The iteration process continues even after delivery of the product where the developer accommodates the field report and users feedback to update the product. The outcome of this stage is a Software Requirement Specification (SRS) document which is basis of all subsequent phases of development.

2.2 DESIGN
In this stage of SDLC process, the developer plans and documents, “how” the set of requirements, as identified in SRS document, be realized. This also includes the architectural issues of the product and user interfaces. The data model (captured as one of the requirements in the requirement analysis phase) is transformed into detailed logical and physical information structure. The output of this phase is the design document containing the product architecture, data flow (both internal as well as external), control flow and process flow.

2.3 IMPLEMENTATION /PRODUCT REALIZATION
The developer in this phase of SDLC converts design details into executable programs for software product. The hardware platform required for the software component of the product is also finalized at this stage. The product prototype along with installation/administration guidance document is the outcome of this phase, which can be taken for testing.

2.4 TESTING
The testing phase requires developers to complete various tests to ensure the accuracy of software code, the inclusion of expected functionality, and the interoperability of applications and other network components.

2.5 DELIVERY
This phase ensures the secure delivery of the product to the end user so that the customer gets the correct system for installation and commissioning.

2.6 MAINTENANCE
The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness. It includes making changes to improve a system’s performance, correct problems, enhance security, or address user requirements.

3. ALIGNMENT OF SDLC IN LINE WITH CC REQUIREMENTS:
Common Criteria standards, in general, take note of generic SDLC process and described its assurance classes. CC also focuses on the overall software development lifecycle processes through its assurance classes like of ‘Life cycle support’. The following table1 summarizes the mapping of general SDLC processes with CC assurance classes

<table>
<thead>
<tr>
<th>Common SDLC phase</th>
<th>CC Assurance classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Requirement Analysis</td>
<td>Security target evaluation</td>
</tr>
<tr>
<td>2 Design</td>
<td>Development</td>
</tr>
<tr>
<td>3 Implementation/Product realization</td>
<td>Development &amp; Lifecycle support (CM, LCD, DVS)</td>
</tr>
<tr>
<td>4 Testing</td>
<td>Tests &amp; Vulnerability Assessment</td>
</tr>
<tr>
<td>5 Delivery</td>
<td>Life cycle support</td>
</tr>
<tr>
<td>6 Maintenance</td>
<td>Life-cycle support (Flaw remediation)</td>
</tr>
</tbody>
</table>
Developing common criteria compliant security products

Table1: SDLC and CC assurance class
The subsequent sections summarize the efforts necessary, by the developer, at different phases of software development life cycle, to make a CC compliant IT security product.

3.1 REQUIREMENT ANALYSIS

3.1.1 Security Target Document
Each product under CC evaluation is attached with a security requirement document called security target (ST). Developer prepares an implementation-dependent statement of security needs for a product and submits it to the evaluation body. Before and during the CC evaluation, the ST specifies “what is to be evaluated”. In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the product and the exact scope of the evaluation. However, after evaluation this document is used by the end users to know “what was evaluated” for a specific product. The end users rely on this document because the product has been evaluated by the evaluators to meet the requirements stated in this document.

EAL1
The CC allows the use of a low assurance ST for an EAL1 evaluation. This low assurance ST is not acceptable for higher level assurance evaluation.

A low assurance Security target contains following information:
- ST Introduction
- Conformance claims
- Security objectives for the operational environment
- Security requirements (Functional and Assurance)
- Security requirements rationale (if dependencies are not satisfied)
- Extended component definition
- TOE summary specification

EAL 2-4
A full Security target contains following information:
- ST Introduction
- Conformance claims
- Security problem definition (threats, organizational security policies, assumptions)
- Security objectives for the TOE and operational environment with rationale
- Extended component definition
- Security requirements (Functional and Assurance) and its rationale
- TOE summary specification

3.2 DESIGN

3.2.1 Functional Specification Document
Developer needs to identify different interfaces of the product. The interfaces include external commands, input data files and output data files used to invoke security features. For each of EAL1 to EAL4 requirements, the depth of functional specification document changes. The details are available in the developer guide document [5].

EAL1
A functional specification document needs to contain following information:
- Purpose, method of use and parameters for each of the interfaces responsible for enforcing or supporting security functions
- Rationale for declaring some of the interfaces as non-interfering for security functions
- Map from security functional requirements as given in ST to the interfaces

EAL2
In the product there may be many other interfaces which are not related to the security functions. However, for EAL2 onwards, these interfaces are also to be described in detail. For EAL2 onwards the functional specification document needs to contain following additional information:
- Purpose, method of use and parameters for each of the all interfaces

EAL3
Users use interfaces, i.e., basically commands or specific inputs to invoke certain security as well as non-security functions. If these inputs directly invoke a security function, then the interfaces are called security enforcing interfaces. For EAL3 onwards the functional specification document needs to contain following additional information:
- Error messages from security function enforcing interfaces

EAL4
Some of the interfaces sometimes support proper operation of security functions, though they may not be used to invoke a security function directly, like a system clock supports timestamps of log data. All these type of security function supporting interfaces are to be considered. For EAL4 onwards the functional specification document needs to contain following additional information:
- Error messages from all security function interfaces, i.e., security function enforcing as well as supporting

3.2.2 Design Document
The design document is prepared by the developer to demonstrate that the security functions are accurately designed and cannot be bypassed during operation of the product.

Requirement for different EAL level
EAL1
For EAL1 this document is not required.
EAL2
In design document, developer needs to identify all subsystems of the product. Some of these subsystems may be directly related to enforce the security functions, whereas, some may support security functions. There may also be subsystems which are not related to any security functions. For EAL2 onwards the design document needs to contain following information:
- Basic design describing the structure of the product
terms of subsystems
• The interactions of the security function enforcing subsystems
• A map from all the interfaces described in functional specification to the behavior of the subsystems described in design document

EAL3
For EAL3 onwards the design document needs to contain following additional information:
• The interactions among the all subsystems of the product

Description of subsystems which are not responsible for security functions to demonstrate that are really not related to security functions.
EAL4
The subsystems of the product may be divided into smaller pieces called modules. For EAL4 onwards the design document needs to contain following additional information:
• Description of the structure of the product in terms of modules.
• Categorization of modules whether a particular module is security-function-enforcing/supporting or non-interfering
• Description of each security-function-enforcing module in terms of its security-function-related interfaces, return values from those interfaces interaction with and called interfaces to other modules.
• Description of all modules in terms of its purpose and interaction with other modules.

3.2.3 Architecture Document
The security product is intended to protect some asset. To provide enough protection to the asset, the product itself is expected to be enough robust. It is expected to have self-protection mechanism through integrity checking, domain separation, i.e., security modules are separated from non-security modules to have less entry points and robust startup procedure to invoke necessary security functions from the beginning of operation.

EAL2
• Basic description of the architecture of the product to understand the security behaviour.
• Demonstration of the property of ‘Self-Protection’, ‘Domain Separation’ and ‘Non-by passability’ through architecture

3.3 IMPLEMENTATION (PRODUCT REALIZATION)
3.3.1 Implementation
In this phase, actual implementation of the product is carried out. Developer writes codes for software product or design circuit diagram for hardware product. Whatever may be the form of implementation; these are to be made available for CC evaluation. Any part of it may be selected by the evaluator for in-depth analysis. The implementation evidences will have correlation with design document of the product. The subsystems which are described in the design document may be taken as baseline and implementation of those may be analyzed by the evaluator. This is required for EAL4 onwards.

3.3.1 Development Security
Developer has to demonstrate that during development of the product, security measures are adequate to provide the confidentiality and integrity of the design and implementation of the product which is necessary to ensure secure operation of the product.[6]

EAL3
For EAL3 onwards the document demonstrating development security needs to contain following information:
• Development security documentation describing all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
(ISO/IEC 27001: Information Security Management System)

3.3.2 Configuration Management
During development and maintenance of the product, developer needs to maintain a secured and controlled environment to minimize security vulnerabilities. Configuration management is one of the aspects for ensuring such environment. If configuration management is in place, the product throughout its build processes can be identified uniquely. Configuration management system can keep track of changes, how changes are incorporated and can also demonstrate degree of automation used for build preparation to reduce the scope of error. The necessary activities for developing IT security products for different EAL compliance in respect of configuration management are as below:

EAL1
• The product is expected to have unique reference number which can be correlated with the number maintained in the configuration management procedure. If it is a software product, it may display its name when made on. For hardware or firmware product, a part number can be given.

EAL2
For EAL2 onwards following additional information may be provided by the developer. These are:
• Developer is expected to keep a documented procedure for configuration management system. In that document developer will identify what are the items are kept under configuration management system and how the items are being identified uniquely throughout its development process and version changes.

EAL3
For EAL3 onwards following additional information may be provided by the developer. These are:
• Configuration management documentation is expected to be elaborated. A configuration management plan may be there. In this plan, developer is expected to
describe how the configuration management system is contributing to prepare the product. Developer is expected to describe product creation, modification, deletion of configuration items as well as data back-up and archiving. Also there may be documentation and evidences to demonstrate only authorized person have access to the product or any other configuration items. Developer may have enough auditing during development and maintenance phase to demonstrate that the configuration items are really kept in the system.

For EAL4 onwards following additional information may be provided by the developer. These are:

- Developer is expected to provide environment to have the production automated. This automated production procedure is required to take constituent components as identified by the configuration management system.

3.4 TESTING
Testing demonstrates that the product behaves as it is intended in its security features specification document. This determination is achieved through tests conducted by the developer known as functional testing and also testing conducted by the evaluator known as independent testing. At the lowest level of assurance (EAL1), there is no requirement of developers’ involvement, so the only testing is conducted by the evaluator. Here, in this paper, we will describe involvement of developer only for different EALs.

EAL1
- No involvement of the developer required for this level of evaluation

EAL2
- From this level onwards developer needs to be involved in testing process. Developer is required to conduct functional testing and produce test documentation. There will be a test plan identifying tests to be carried out. Test scenarios are also to be described. Test environment, test procedure, ordering dependency, expected result and actual results are to be described with the aim that the test can be repeatable. For identification of test scenarios, developer needs to refer its security target and functional specification document.
- Test scenarios are expected to be drawn from security target as well as functional specification for the product. Developer has to include interfaces like external commands related to security, input data file, output data file as mentioned in the functional specification document for generating test scenarios.

For EAL3 onwards following additional information may be provided by the developer. These are:
- Test scenarios are expected to be drawn from security target as well as functional specification for the product. Developer has to judiciously include all interfaces like external commands related to security, input data file, output data file as mentioned in the functional specification document for generating test scenarios.

- Test scenarios are also to be drawn from design document considering interactions of subsystems.

For EAL4 onwards following additional information may be provided by the developer. These are:
- Test scenarios are to be drawn from design document considering all interactions of subsystems.

3.5 SECURE DELIVERY OF PRODUCT TO THE END USER
It is expected that the developer follows documented and controlled procedures to deliver the product from development environment to the end-user. The procedures will be such that the product is not compromised during packaging, storage and distribution. There may be procedure that the end-user will be able to verify integrity of the product. If confidential delivery is required, then sealed envelope can be used. If the product is a software product then encryption also can be used. If availability is of concern, then a secured transportation is required. This document is required from EAL2 onwards.

3.6 Post Maintenance and patch management
Developer may follow controlled and documented procedures for patch management and can have augmented evaluation with EAL+ mark. This is not mandatory for any EAL, however, often it is adopted by developers for augmented evaluation. The degree of patch management can vary. The necessary document is required to describe tracking of each security flaw in each release of the product. In this tracking, developer may indicate procedures to identify the flaw, nature of flaw, impact of flaw, reason and remediation of the flaw etc.

4. CC EVALUATION OF IT SECURITY PRODUCT
The developer produces the product and submits it to the evaluation body as target of evaluation (TOE) and is responsible for providing the evidence required for the evaluation( product related document such ST, FSP, Design, Architecture, Test, Guidance and process related document such as CM system, Life cycle model, delivery etc). The evaluators in the CC Test laboratory (CCTL) perform the evaluation tasks required in the context of an evaluation: the evaluator receives the evaluation evidence from the developer, performs the evaluation sub-activities and provides the results of the evaluation assessment in the form evaluation technical report (ETR) to the certification authority. The evaluator acquires an in-depth knowledge of the construction of the product by examining the required security functions and tracing the security functionality to lower levels of design or implementation. In addition, depending on the assurance level, the evaluators examine how guidance is given to administrators and users, how the product is developed, and how vulnerable the product is to attack.

4.1 EVALUATION OF PRODUCT RELATED DOCUMENT
The evaluators review the security target (ST) document for its compliance with the CC standards part I for structure and contents of the documents, CC part II for security functional requirements and CC part III for security assurance requirements. In order to maintain the repeatability and reproducibility of the evaluation results the evaluators may design and use checklists in line with work unit wise analysis of each requirement as defined in CEM. The evaluators verifies unique identification of the TOE and ST , the compliance statement in regards to PP and any assurance package claim, security problem definitions, Security functional requirements , assurance requirements, TOE summary specification ,over all internal and external consistency, rationale , document versions etc. This review generally undergoes several iterations unless all the requirements are met. The evaluated ST document is published in the CC portal for use by the consumer, it should be written in manner so that the consumer can get necessary information about the product features and application hints.

Functional specification (FSP) document is the next level of product documentation which identifies the Toe security function (TSF) interfaces (TSFI). The TSFIs are means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF. The evaluators review the FSP document to verify the compliance to CC part III for development security assurance requirements. The FSP document should map all the security functional requirements as identified in the ST document. Functional specification (FSP) is an important development document which enables the evaluator to understand the security architecture in terms of self protection and bypassability, designing test cases, and searching vulnerability of the product.

The goal of design documentation is to provide sufficient information to determine the TSF boundary, and to describe how the TSF implements the Security Functional Requirements in the product. The amount and structure of the design documentation will depend on the complexity of the TOE and the number of SFRs. The design document should describe the subsystem level and modular level details for realization of the SFRs as applicable for different targeted evaluation assurance levels (EAL).The CC evaluation process is depicted in the fig 2.

**Figure 2: CC evaluation process**

For the secure preparation and operation of the TOE it is necessary to describe all relevant aspects for the secure handling and configuration of the TOE. The guidance document also addresses the possibility of unintended incorrect configuration or handling of the TOE.

### 4.2 EVALUATION OF THE DEVELOPMENT PROCESS RELATED DOCUMENTS

The security of an ‘IT security product’ depends not only on the security functionalities, it is offering, but also how those are implemented in the product. The development process plays important role to give confidence and assurance to the user community regarding the product security. The processes are related to configuration management (CM), development security, life cycle model, delivery, tools and techniques, flaw remediation. Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance. Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development and maintenance activities.

CM systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorized, in turn it reduces the likelihood that accidental or unauthorized modifications.

The requirements for secure delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE to the user.

Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE and its parts. It includes the physical security of the development location and any procedures used to select development staff.

The developer should establish the development processes so that product integrity is maintained through CM system, security of the distribution is maintained so that the consumer get the evaluated version of the product in a secure channel and
any correction or fixes afterward are forwarded to the end user in a secure manner and, controlled development is done through some established life cycle model for higher assurance claim. The reviewer evaluates the process documents to see the compliance against relevant CC part III clauses.

4.3 TESTING OF THE IT SECURITY PRODUCT
Testing the product is carried out by the developer as a confirmation that the TSF operates according to its design descriptions and identified security features in the ST document and prepare test documentation. The testing provides the assurance that the likelihood of undiscovered flaws is relatively small. The evaluators reconfirm the tests by execution of some test cases already done by the developer and do additional tests independently. The evaluators devise the test plan, test procedure and record all the test condition, expected results and the actual results.

4.4 VULNERABILITY ANALYSIS OF IT SECURITY PRODUCT
The Vulnerability assessment addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE. Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorized access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorized capabilities of other users. The evaluators search the evaluation evidences submitted by the developer for any vulnerability as well as search the publicly available sources for any reported vulnerability of similar type of products. Then the evaluators calculate the attack potential of the identified vulnerabilities. If the attack potential is more than the limit that the product of particular EAL level can withstand then that vulnerability becomes a candidate for penetration testing to exploit the vulnerability.

4.5 SITE VISIT OF THE DEVELOPMENT / DISTRIBUTION AREA
As a part of CC evaluation the evaluators also visit the development and distribution site of the developer to assess the configuration management system being implemented there, delivery of products and development security depending on the EAL level [2].

CONCLUSIONS
Common criteria are a useful standard for the development of products and systems with IT security functions and also a guide for procurement of commercial products and systems with in-built security functions. Developers may refer this paper to align their development process and develop product and process documents as per CC standards. Developers wishing to develop CC compliant IT security product need to specify their products security features and functions correctly in the ST document and then follow the controlled and disciplined product development process to realize the product aligning the ST document. The developer needs to produce various products and process related documents throughout the life-cycle as evaluation evidence which will add confidence to the user community. If the developers follow the requirements as specified in the CC standards for development of IT security product the goal of confidence in implemented security measures in the products will be achieved.

FUTURE SCOPE
The common criteria test lab (CCTL) of STQC IT services, Kolkata is presently carrying out CC evaluation of different IT security products under the Indian national scheme “Indian Common criteria certification scheme (IC3S)” run by STQC certification cell. At present India is a member of CCRA (common criteria recognition arrangement), an international body, as CC certification consuming nation. STQC is in the process of International recognition as a certificate authorizing country under CCRA programme.

ACKNOWLEDGEMENT
The authors acknowledge the active support and guidance received from Smt. Mitali Chatterjee, Sr. Director STQC, IT services, Kolkata.

REFERENCES
[1] Common criteria standards ISO/IEC 15408 part 1, 2, 3