Common Criteria
(CC)

The Common Criteria (CC) evaluation methodology has three components: the CC documents, the CC Evaluation Methodology (CEM), and a country-specific evaluation methodology called an Evaluation Scheme or National Scheme. The CC evolved from the TCSEC, FIPS, ITSEC (United Kingdom, France, Germany, and the Netherlands), CTCPEC (Canada), and various other international and national organizations. The CC became the de facto security evaluations standard in the United States in 1998.

Overview

1. CC Documents
2. CC Evaluation Methodology
3. Country specific evaluation methodology

Def: A Target of Evaluation (TOE) *Security Policy* (TSP) is a set of rules that regulate how assets are managed, protected, and distributed within a product or system.

Def: The TOE *Security Function* (TSF) is a set consisting of all hardware, software, and firmware of the product or system that must be relied upon for the correct enforcement of the TSP.

Note: The TSF is a generalization of the TCSEC concept of a TCB.

The CC supports two kinds of evaluations: evaluations of protection profiles and evaluations of products or systems against security targets. Product evaluations are awarded at one of seven predefined Evaluation Assurance Levels (EALs).

There are two kinds of evaluations:

Def: A CC *protection profile* (PP) is an implementation-independent set of security requirements for a category of products or systems that meet specific consumer needs.

The PP describes a family of products.

Def: A *security target* (ST) is a set of security requirements and specifications to be used as the basis for evaluation of an identified product or system.

The ST addresses security issues relative to a specific product, not a family of products.

The Protection Profile (PP) consists of:

1. Introduction

2. Product or system family description

3. Product or system family security environment
    - assumptions about intended usage and environment of use
    - threats, type of attacks, and targets of attack
    - organizational security policies

4. Security objectives
    - traced back to identified threats/policy
    - traced back to threats/policies not completely countered by product

5. IT security requirements
    - functional and assurance requirements

6. Rationale
    - objectives and requirements
    - objectives traceable to assumptions, threats, and policies
    - requirements traceable to objectives and how they are met

The security target (ST) consists of

1. Introduction
    - identification, overview, conformance claim

2. Product or system description

3. Product or system family security environment
    - assumptions, usage, and environment
    - threats
    - original security policies

4. Security objectives
    - traced back to threats, original security policies not completely addressed

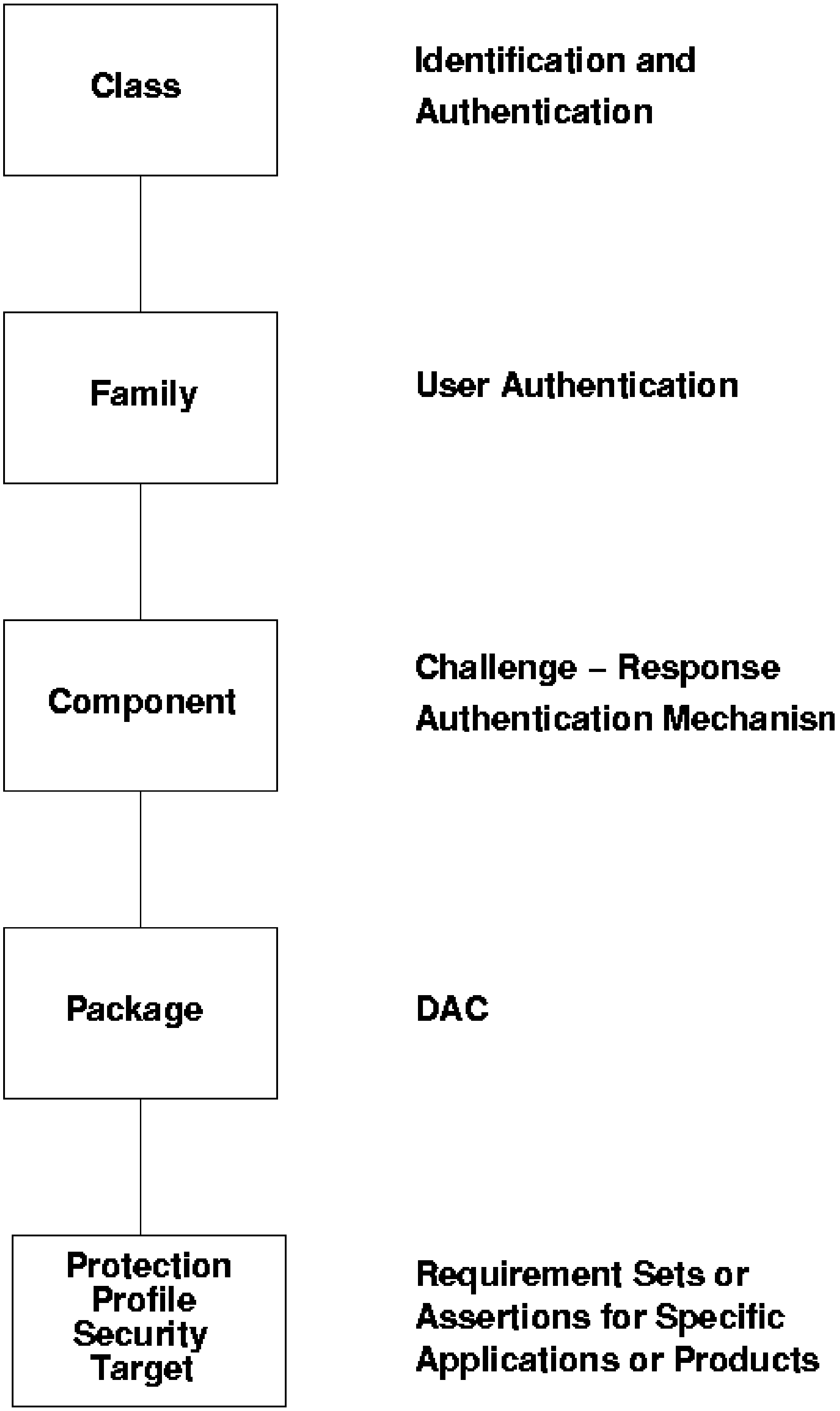
5. IT Security Requirements
    - functional & assurance requirements

6. Product or system summary specification
    - security functions & how they address requirements
    - assurance and how are met

7. PP Claims

8. Rationale
    - security objective rationale
    - security requirements rationale
    - TOE summary requirements & specification rationale
    - rationale for not meeting all requirements
    - PP Claims rationale

Evaluation



Class — Identification and Authentication

Family — User Authentication

Component — Challenge – Response Authentication Mechanisn

Package — DAC

Protection Profile Security Target — Requirement Sets or Assertions for Specific Applications or Products

Security Functional Requirements

The heart of the CC is the requirements themselves. The CC defines both functional and assurance requirements and then builds EALs out of the assurance requirements. There are 11 classes of security functional requirements. The classes are given in the table below:

Functional Requirements

11 Classes

FAU – Security Audit	6 Families
FCO – Communications	2 Families
FCS – Cryptographic Support	2 Families
FDP – User Data Protection	13 Families
FIA – Identification and Authentication	6 Families
FMT – Security Management	6 Families
FPR – Privacy	4 Families
FPT – Protection of Security Functions	16 Families
FRU – Resource Utilization	3 Families
FTA – TOE Access	6 Families
FTP – Trusted Path	2 Families

There are ten security assurance classes. One relates to the protection profile, one to the security targets, one to the maintenance of assurance and the remainder to the product or system. The assurance requirements are given in the table below:

Assurance Requirements

10 Classes

APE – Protection Profile Evaluation	6 Families
ASE – Security Target Evaluation	8 Families
ACM – Configuration Management	3 Families
ADO – Delivery and Operation	2 Families
ADV – Development	7 Families
AGD – Guidance Documentation	2 Families
ALC – Life Cycle	4 Families
ATE – Tests	4 Families
AVA – Vulnerabilities Assessment	4 Families
AMA – Maintenance of Assurance	4 Families

Level of Assurance

The CC has seven level of assurance. They are given below in increasing level of assurance.

EAL1: Functionally Tested

EAL2: Structurally Tested

EAL3: Methodically Tested and Checked

EAL4: Methodically Designed, Tested, and Reviewed

EAL5: Semi-formally Designed and Tested

EAL6: Semi-formally Verified, Designed, and Tested

EAL7: Formally Verified, Designed, and Tested

The table below depicts the correspondence between the TCSEC and the CC.

TCSEC	**CC**
D	---
---	EAL1
C1	EAL2
C2	EAL3
B1	EAL4
B2	EAL5
B3	EAL6
A1	EAL7

Evaluation Process

The CC evaluation process is performed by NIST-accredited commercial laboratories that do evaluations for a fee. Typically, a vendor selects an accredited laboratory to evaluate a Protection Profile or a product or system. The laboratory performs the evaluations on a fee basis. When the Protection Profile evaluation is complete, the laboratory presents its findings to the validating agency. That agency decides whether or not to validate the Protection Profile evaluation and award the EAL rating.

Evaluation of a product or system is slightly more complex because there are more steps involved and more evaluation evidence deliverables. A draft of the product or system security target must be provided before the laboratory can coordinate the project with the validating organization. When the product or system evaluation is complete, the laboratory presents its findings to the validating agency. That agency decides whether or not to validate the product or system evaluation and award the EAL rating.