FEDERAL CRITERIA

for

INFORMATION TECHNOLOGY SECURITY

VOLUME II

Registry of Protection Profiles

Version 1.0

December 1992

This document is undergoing review and is subject to modification or withdrawal. The contents of this document should not be referenced in other publications.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
&
NATIONAL SECURITY AGENCY

NOTES TO REVIEWERS

This is the first public draft of work in progress by the joint National Institute of Standards and Technology (NIST) and National Security Agency (NSA) Federal Criteria (FC) Project. This draft *Federal Criteria for Information Technology Security* is provided for preliminary review and comment by members of the national and international computer security community. The document will evolve into a new Federal Information Processing Standard (FIPS) intended principally for use by the United States Federal Government, and also by others as desired and appropriate. The FIPS is intended to replace the *Trusted Computer System Evaluation Criteria (TCSEC)* or "Orange Book."

Our objectives in presenting this draft material are threefold: first, to give the community a clear view of the FC Project's direction in moving beyond the TCSEC method of expressing requirements in order to meet new IT security challenges; second, to obtain feedback on the innovative approaches taken, the method of presentation, and granularity; and third, to make a substantial contribution to the dialogue among nations leading to the harmonization of IT security requirements and evaluations.

It is important to note a few things about this preliminary FC draft. First, it is a new and unpolished document and not intended for any purpose except review and comment. Organizations should not adopt any contents of this draft document for their use. It is anticipated that the document will undergo extensive revision as it works its way through the public FIPS approval process over the next year or two. Second, the FC is being distributed in two volumes. Volume I addresses the criteria development process and is intended principally for use by developers of protection profiles. The information in Volume I may also be of use to IT product manufacturers and product evaluators. Volume II presents completed IT product security criteria in the form of accepted protection profiles.

The protection profiles associated with the final FIPS will help consumers identify types of products that meet the protection requirements within their particular organizations and environments. However, the FIPS will be supplemented by a series of implementing guidance documents, many of which will be designed to help consumers make cost-effective decisions about obtaining and appropriately using security-capable IT products.

As a preliminary draft of the new FC-FIPS, this document is not intended for general distribution or compliance. The document should not be considered a complete or finished product. Your comments will be used by the Federal Criteria Working Group to help raise the maturity level of this material prior to being circulated for further public comment in the FIPS development process.

ADDITIONAL NOTES TO REVIEWERS

Reviewers who provide substantive comments on the enclosed draft FC by March 31, 1993 will be invited to attend an Invitational Workshop on the Federal Criteria. This two-day workshop will be held in the last week of April 1993 in the Washington-Baltimore area at a location to be announced. All comments received by the cut-off date will be correlated into major themes for discussion by break-out groups at the workshop. The results will be used as input into the process of re-drafting the FC for a second round of comment prior to its being formalized as a FIPS.

Please send your comments (electronic format preferred) to **Nickilyn Lynch** at the U.S. National Institute of Standards and Technology (NIST), Computer Systems Laboratory (CSL).

Phone: **(301) 975-4267**
FAX: **(301) 926-2733.**

(Internet) Electronic Mail:

lynch@csmes.ncsl.nist.gov

Postal or Express Mail
(Hardcopy or 3.5”, 1.44M diskette in MSDOS, Macintosh, or Sun format):

Federal Criteria Comments
Attn: Nickilyn Lynch
NIST/CSL, Bldg 224/A241
Gaithersburg, MD 20899

Sincerely,

Eugene F. Troy
NIST Co-Manager
Federal Criteria Project

Ron S. Ross
NSA Co-Manager
Federal Criteria Project

NIST National Institute of Standards and Technology
Gaithersburg, MD 20899

COMMERCIAL SECURITY REQUIREMENTS
FOR
MULTI-USER OPERATING SYSTEMS

A family of Protection Profiles for the
Federal Criteria for Information Technology Security

Issue 1.1
January 1993
Supersedes Minimum Security Requirements
for Multi-User Operating Systems

Computer Security Division
Computer Systems Laboratory
National Institute of Standards and Technology

Chapter 1.

CS2 Functionality

Chapter 1.
Commercial Security Requirements (CSR)

1.1 Introduction

Government and commercial institutions rely heavily on information technology (IT) products to meet their operational, financial, and information requirements. The corruption, unauthorized disclosure, or theft of electronically-maintained resources can have a disruptive effect on an organization's operations as well as serious and immediate financial, legal, and public confidence impact.

Products conforming to the Commercial Security (CS) requirements contained in this document are intended to be useful to a broad base of users in the private, civil government, and defense sectors. This includes application developers, end users, and system administrators. The Protection Profiles specified in this document provide organizations with three set of security requirements, defined as CS1, CS2, and CS3, with CS3 offering the highest degree of trust.

The Protection Profiles as a whole specify “baseline” requirements that meet generally accepted security expectations for a class of products colloquially called “general purpose, multi-user operating systems.” These requirements apply to multi-user workstations, minicomputers, and mainframes. Most required mechanisms are configurable so that customers can satisfy their unique security policies and objectives.

The intent of the Protection Profiles is to promote the wide availability of products possessing security enforcing functions that are of such broad applicability and effectiveness that they become part of the “normal” mode of operation. It is anticipated that vendors will respond to user expectations by increasing the availability of operating systems that meet these general security requirements. These requirements represent the integration of a number of security requirement specifications from various sources into a single set that is expected to have wide acceptance.

1.1.1 CS Description

The Protection Profiles address the security features and their development. The Protection Profiles were written to meet several objectives: to serve as a "metric" for the amount of security present in a computer system processing sensitive information; to provide guidance to the developers as to what security features to build into their planned products; and to provide a method for uniformly specifying security requirements in acquisition specifications.

The CS requirements are divided into three hierarchical Protection Profiles. The profiles are CS1, CS2, and CS3, with C3 providing the greatest degree of security. Each profile represents a level of trust that can be placed in a product and specifies a collection of requirements in the form of features and assurances. Each profile includes most of the features and assurances of the previous profile along with additional, more stringent features and assurances. The reasoning for requirements leveling for each Protection Profile can be found in the rationale in Chapter 2. This reasoning is based on the overall effectiveness of each Protection Profile in addressing the threats identified in that chapter.

The Protection Profiles specify computer-based protection mechanisms for the design, use, and management of information systems. The Protection Profiles include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information sharing computer systems. CS-conformant computer products provide system administrators with tools to control the sharing of information and resources based primarily on the identity of users, or, in the case of CS3, the role associated with the user, as well as the time of day, terminal location, or type of access requested. The technical measures also provide tools to protect against both common user actions that may compromise security and against deliberate penetration attempts by "hackers." In addition, there are requirements to log events that may impact the security of either the product or the information that it is processing. All functionality requirements are based on existing and well understood security practices.

1.1.2 Background

These Protection Profiles have been developed by the CS Working Group of the Federal Criteria Project under NIST leadership with a high level of private sector participation. They are based on the Trusted Computer System Evaluation Criteria (TCSEC) [1] C2 criteria class, with additions from current computer industry practice, from commercial security requirements specifications, and from the on-going work of the Federal Criteria Project. Their development has also been guided by international security standards efforts and by the recommendations of the System Security Study Committee.

The following sub-sections provide descriptions of each of these sources, and gives further background on the motivation for and development of the Protection Profiles.

1.1.2.1 Trusted Computer System Evaluation Criteria (TCSEC)

The TCSEC [1], originally published in 1983 and revised in 1985, was the first publicly available document that expressed general security requirements that could apply to a specific class of technology (e.g., operating systems). It represents the culmination of many years of effort to address Information Technolgy (IT) security issues within the Department of Defense (DoD) classified world. The TCSEC is made up of IT security features and assurances that have been derived and engineered to support a very specific DoD security policy - the prevention of unauthorized disclosure of classified information (i.e., confidentiality).

During the past few years, commercial enterprises and government organizations processing sensitive information have begun to pay increasing attention to IT security needs. Although the TCSEC-motivated security features have proven valuable in addressing their security problems, often these features have been viewed as less than perfect and incomplete and only to have been specified because a more appropriate set of security functions has not been available.

The Protection Profiles are intended to be the first step in “filling this gap” by providing a set of security requirements appropriate for commercial enterprises and government organizations concerned with protecting sensitive information.

1.1.2.2 Commercial Security Efforts

Recognizing that the TCSEC was a valuable starting point, but not sufficient for their security needs, two commercial companies - Bellcore and American Express Travel Related Services (TRS) - independently initiated efforts to develop security requirements for their environments. At Bellcore, these efforts resulted in a *Bellcore Standard Operating Environment Security Requirements* [3] document and at TRS the efforts resulted in the internal *C2-Plus* company security standard.

The Bellcore document was developed to meet the security needs of Bellcore and its client companies, the Regional Bell Operating Companies (RBOCs). The requirements specified in the Bellcore document were derived both from commonly recurring security requirements for RBOC computer applications and from experiences of Bellcore's computer security assessment group.

In developing the *C2-Plus* document, TRS found that, while the TCSEC met many requirements of the commercial sector, the prescribed features at the C2-level (and its F2-level counterpart in the ITSEC [2]) fell short in several areas that were either introduced at higher TCSEC levels or were not addressed at all in the respective standards. Consequently, the TRS document was developed as an enhanced, commercialized version of the C2-level security requirements of the TCSEC.

Using the TRS document as input, the International Information Integrity Institute (I-4), a consortium of large international corporations, developed the *Commercial International Security Requirements (CISR)* [4]. The rationale for the development of the CISR include the following:

> "Military-oriented information security requirements (i. e., TCSEC) are not suitable in many respects for the needs of international businesses." [4]

The final version of the CISR was published in April 1992.

1.1.2.3 System Security Study Committee

The System Security Study Committee was formed in 1988 in response to a request from the Defense Advance Research Projects Agency (DARPA) to address the security and trustworthiness of U.S. computing and communications systems. The Committee, which was composed of 16 individuals from industry and academia, including computer and communications security researchers, practitioners, and software engineers, was charged with developing a national research, engineering, and policy agenda to help the United States achieve a more trustworthy computing technology base by the end of the century. In 1991, the Committee published the *Computers at Risk* [5] report, which presents the Committee's assessment of key computer and communications security issues and its recommendations for enhancing the security and trustworthiness of the U.S. computing and communications infrastructure.

The development of the Protection Profiles was guided by one of the recommendations from this report that:

> "...a basic set of security-related principles for the design, use, and management of systems that are of such broad applicability and effectiveness that they ought to be a part of any system with significant operational requirements" [5] should be developed.

1.1.2.4 Minimum Security Functionality Requirements (MSFR)

The second draft of the Minimum Security Functionality Requirements for Multi-User Operating Systems (MSFR) [10] was published in January of 1992. The MSFR was developed as part of a project to stimulate the development of IT products broadly useful to the diverse security needs of the US Government (civilian and military) and the private sector.

The MSFR specified the minimum level of security that NIST and NSA felt should be available in any commercially available multi-user operating system. The MSFR represents an extension of the TCSEC controlled access protection class, level C2, with additions based on current industry practice and security requirements specifications developed in the commercial environment. Much of the MSFR is derived from the TCSEC, the *Bellcore Standard Operating Environment Security Requirements*, and the CISR with overall guidance from the *Computers at Risk* report [5].

1.1.2.5 Commercial Security (CS) requirements

To help support the Federal Criteria, the CS Working Group was tasked with developing a family of Protection Profiles, based on an updated version of the MSFR. The three Protection Profiles included in this document have been developed in compliance with the prescribed approach and format of the Federal Criteria [11]. Components of the Federal Criteria were selected for each Protection Profile and were enhanced with refinements and assignments that were taken from the November 1992 version of the MSFR. The Protection Profiles are intended to satisfy the most common security needs of computer system users.

1.1.3 Document Organization

Chapter 1 (this chapter) provides introductory and background information. The rest of this document is divided into three Protection Profiles, CS1, CS2, and CS3. The development of these Protection Profiles are in accordance with the Protection Profile format specified by the Federal Criteria. Chapter 2 provides the rationale for the selection of the security features and assurance evidence. This rationale also includes descriptions of the intended use of the product, the environmental assumptions that were made for a CS-compliant system, and the expected threats. Chapter 3 specifies the security functionality that a CS-compliant system is required to provide, and Chapter 4 specifies the assurance requirements. At the end of the CS requirements, there is a Glossary and a list of references.

COMMERCIAL SECURITY 1 (CS1)

Products that comply with this Protection Profile provide access control capabilities to separate users and data based on finely grained access controls. It incorporates credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect sensitive information and to keep other users from reading or destroying their data. Users are individually accountable for their actions through login procedures, auditing of security relevant events, and resource isolation. This CS1 Protection Profile is equivalent to a Class C2 - Controlled Access Protection from the TCSEC [1]. It consists of TCSEC requirements plus those evaluation interpretations that a product must meet before it can be evaluated at the C2 level.

COMPONENT SUMMARY:

CS1 Functional Component Summary

Component Name	Component Code	Level
Security Policy Support:		
Identification & Authentication	I&A	1
Audit	AD	1
Access Control	AC	1
Reference Mediation	RM	1
TCB Protection	P	1
Self Checking	SC	1

CS1 Assurance Package Summary

Assurance Component Summary	T1
Development Process	
TCB Property Definition	PD-1
TCB Design	
TCB Element Identification	ID-1
TCB Interface Definition	IF-1
TCB Modular Decomposition	----
TCB Structuring Support	----

CS1 Assurance Package Summary

Assurance Component Summary	T1
TCB Design Disciplines	----
TCB Implementation Support	----
TCB Testing & Analysis	
Functional Testing	FT-1
Penetration Analysis	---
Covert Channel Analysis	----
Operational Support	
User’s Security Guidance	UG-1
Administrative Guidance	AG-1
Flaw Remediation	---
Trusted Generation	---
Development Environment	
Life Cycle Definition	----
Configuration Management	---
Trusted Distribution	----
Development Evidence	
TCB Protection Properties	EPP-1
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	---
Covert Channel Analysis	----
Product Support	---
Evaluation Process	
Testing	
Test Analysis	TA-1
Independent Testing	IT-1
Review	
Development Environment	---
Operational Support	OSR-1
Analysis	
Protection Properties	---
Design	---
Implementation	---

CS1 Rationale

2.2 Introduction

As outlined in the Federal Criteria, this rationale describes the protection philosophy, how the security features are intended to be used, the assumptions about the environment in which a compliant product is intended to operate, the threats within that environment, and the security features and assurances that counter these threats.

The level of components that were chosen for the CS1 Protection Profile are equivalent to Class C2 of the TCSEC [1]. They consist of TCSEC requirements plus those evaluation interpretations that a product must meet before it can be evaluated at the C2 level.

2.2.1 Protection Philosophy

Any discussion of protection necessarily starts from a protection philosophy, i.e., what it really means to call the product “secure.” In general, products will control access to information and other resources through the use of specific security features so that only properly authorized individuals or processes acting on their behalf will be granted access. For CS1, three fundamental requirements are derived for this statement of protection:

- Access authorization
- Accountability
- Assurance

The totality of the functionality that enforces the access authorization and accountability protection philosophy is comprised of the hardware, software, and firmware of the Trusted Computing Base (TCB). CS1 requires the TCB to be protected from external interference and tampering so that it is effective at countering identified threats. The assurance protection philosophy is comprised of the development process, operational support, development evidence, and evaluation process assurances. Each of these are explained below.

2.2.1.1 Access Authorization

The access authorization portion of the philosophy of protection for this profile addresses subject and object access mediation. CS1 provides protected access to resources and objects. As defined in the TCSEC and specified in this profile, access control permits system users and the processes that represent them to allow or disallow to other users access to objects under their control:

> Access control is "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject." [1]

These controls permit the granting and revoking of access privileges to be left to the discretion of the individual users.

2.2.1.2 Accountability

The accountability portion of the philosophy of protection for this profile addresses user Identification and Authentication (I&A) and requirements for security auditing. Each of these are explained below.

2.2.1.2.1 Identification and Authentication

User identification is required to support access control and security auditing. This includes the capability to establish, maintain, and protect a unique identifier for each authorized user. User identification is functionally dependent on authentication. Authentication is a method of validating a person as a legitimate user.

2.2.1.2.2 Audit

For most secure products, a capability must exist to audit the security relevant events. As each user performs security relevant tasks, the product must record the user identifier, the action performed, and the result in a security log. For CS1 compliant products, a capability is specified to allow a system administrator to access and evaluate audit information. This capability provides a method of protection in the sense that security relevant events that occur within a computer system can be logged and the responsible user held accountable for his/her actions. Audit trails are used to detect and deter penetration of a computer system and to reveal activity that identifies misuse.

CS1 provides for an effective audit mechanism by supporting the following basic security characteristics. It provides the ability to:

- review the use of I&A mechanisms;
- discover the introduction of objects into a user's address space;
- discover the deletion of objects; and
- discover actions taken by computer operators and system administrators.

2.2.1.3 Assurance

Assurance addresses threats and vulnerabilities that can affect the product during its development and it addresses evaluation assurance. Assurance Package T1 was selected for the CS1 level. This minimal assurance level is intended to include most commercial computer products that incorporate protection components today. Minimal assurance refers to the fact that this package includes the lowest levels of development and evaluation assurance components and only those components deemed important to provide the necessary minimal understanding of the product.

The intent of the product development assurance for this package is to establish that the external behavior of the product conforms to its user level and administrative documentation without any analysis of the internal structure of the product's TCB. For this reason, only the claimed TCB protection properties, TCB interface description, and TCB element list are required to enable security functional testing.

The intent of the operational support assurance for this package is to establish a minimal level of user and administrative guidance and product information that enables the correct product installation, use of product security features, and remediation of flaws.

The development evidence is commensurate with the assurances required. The intent is to require the type of assurance evidence that is generated during the normal commercial development process.

Evaluation support assurance establishes that the product, and the context in which it is developed and supported, is commensurate with the development assurance requirements. At the T1 level, testing analysis and the requirement for independent testing determines whether the product minimally meets the functional protection requirements. Operational support evaluation assurance determines whether the product documentation correctly describes the security relevant operations.

2.2.2 Intended Method of Use

All individual users (both administrative and non-administrative) are assigned a unique user identifier. This user identifier supports individual accountability and access control. The operating system authenticates the claimed identity of the user before allowing the user to perform any further actions.

A CS1 compliant product imposes controls on authorized users and on processes acting on their behalf to prevent users from gaining access to information and other resources for which they are not authorized. The product provides the capability for users to allow or disallow to other users access to objects under their control. The objects are files that may be read or written to or programs which may be executed. The granularity of control is to the level of individual users (although groups made up of individual users may be specified) and individual objects. CS1 access controls permit the granting and revoking of access to be left to the discretion of the individual users.

Products that comply with CS1 specifications are intended to be used within the following operational constraints:

- The information system is designed to be administered as a unique entity by a single organization.
- The information system is designed to manage computing, storage, input/output, and to control the sharing of resources among multiple users and computer processes.
- The administrative and non-administrative users are identified as distinct individuals.
- The granting and revoking of access control permissions are left to the discretion of individual users.
- The information system provides facilities for real-time interaction with users that have access to input/output devices.

2.2.3 Environmental Assumptions

A product designed to meet the CS1 Protection Profile is intended to be a general purpose, multi-user operating system that runs on either a workstation, minicomputer, or mainframe. CS1 compliant products are expected to be used in commercial and government environments. For government environments, CS1 conforms to the TCSEC C2 class of trust [1].The information being processed may be unclassified, sensitive-but-unclassified, or single-level classified, but not multi-level classified information.

The following specific environmental conditions have been assumed in specifying CS1:

- The product hardware base (e.g., CPU, printers, terminals, etc.), firmware, and software will be protected from unauthorized physical access.
- There will be one or more personnel assigned to manage the product including the security of the information it contains.
- The operational environment will be managed according to the operational environment documentation that is required in the assurance chapter of the Protection Profile.
- The IT product provides a cooperative environment for users to accomplish some task or group of tasks.
- The processing resources of the IT product, including all terminals, are assumed to be located within user spaces that have physical access controls established.

2.2.4 Expected Threats

In general, the choice of which Protection Profile to choose depends upon the level of security that is required for that particular organizational environment. The lowest level, the CS1 level, is intended for those commercial and government environments where all the system personnel are trusted and all the data on the system is at the same classification level. For example, a government agency where all personnel has a government clearance, all data is unclassified, and there is no outside network connections would be an ideal candidate for CS1, i.e., the threats to be countered are such that only a minimal level of trust is needed. However, most commercial and government environments are more complex and require a higher degree of trust. CS2 addresses the security needs for the mainstream commercial and government environments. It provides a higher level of trust for those organizations that need to enforce a security policy where there is no need for different classifications of data. CS3 is intended to provide the highest level of trust for commercial and government environments. It is intended to be used in those environments where a great deal of trust is required, such as in law enforcement agencies, nuclear facilities, or commercial airports. It provides the strongest features, mechanisms, and assurances to counter these threats.

A product that is designed to meet the CS1 Protection Profile and operate within its assumed environment will provide capabilities to counter threats. It should be noted, however, that although a product may faithfully implement all the features and assurances specified in this Protection Profile, the complete elimination of any one threat should not be assumed.

The following threats have been assumed in specifying this CS1 Protection Profile:

1. AN UNAUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO THE SYSTEM

For CS1 compliant products, the threat of an unauthorized user gaining access to the system is primarily addressed by I&A. I&A features allow the TCB to verify the identity of individuals attempting to gain access to the system. This is accomplished through the use of passwords.

Although not a direct countermeasure, auditing requirements are specified at the CS1 level to provide the capability to perform an after-the-fact analysis of unauthorized system entry and login attempts. This provides an opportunity for the system administrators to take corrective actions, such as strengthening existing user authentication methods or requiring users to change their passwords.

2. AN AUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO RESOURCES WHEN THE USER IS NOT ALLOWED ACCESS

An authorized user can try to gain access to unauthorized resources by assuming the user identifier of another user and thus gaining their associated access rights. This is addressed through the use of passwords.

Once an authorized user has gained access to the system, the threat still remains for a user to gain access to resources when the user is not authorized. At the resource level, CS1 specifies access control features to mediate (i.e., distribute, review, and revoke) user access to a subset of resources.

The object reuse feature has been specified to ensure that resource contents are cleared before they are reused. This reduces the vulnerability that the resource contents can be read before it is overwritten.

3. SECURITY RELEVANT ACTIONS MAY NOT BE TRACEABLE TO THE USER ASSOCIATED WITH THE EVENT

CS1 accountability and audit requirements are specified to provide the capability to track security relevant actions performed by users and link such actions, if possible, to the responsible identifier. Audit mechanisms are responsible for the monitoring and detecting of real or potential security violations or events. These audit events can include successful or unsuccessful: I&A events, the introduction of objects into a user's address space, the deletion of objects, and actions taken by system administrators. Each audit record includes the date, time, location, type of event, identity of the user and object involved, and the success or failure of the event.

4. SECURITY BREACHES MAY OCCUR BECAUSE OF TCB PENETRATION

TCB protection is a fundamental capability of CS compliant products. The security components and mechanisms described in this Protection Profile depend upon the integrity of the TCB and on the TCB being isolated and non-circumventable. CS1 specifies requirements for a common and basic set of security features to protect the TCB from outside penetration.

This threat is also countered through product assurance. TCB interface definition establishes the boundary between the TCB and its internal users. Security functional testing establishes that these TCB definitions and properties satisfy the requirements of this Protection Profile.

5. USERS MAY BE ABLE TO BYPASS THE SECURITY FEATURES OF THE SYSTEM

This threat is countered by authentication, access control, audit, TCB isolation, TCB non-circumventability, and reference mediation requirements. Authentication requirements protect authentication data from unauthorized users. Resource access control requirements protect access control data.

Audit requirements provide for the logging of successful and unsuccessful accesses to resources as well as for changes made to the system security configuration and system software in the event that the system security features have been bypassed.

The CS1 specification for reference mediation protects the integrity of the access control mechanism and the TCB's functionality. Starting at CS1, requirements exist for TCB mediation of user references to objects and to security relevant services.

CS1-compliant products maintain a domain for its own execution to protect it from external interference and tampering. Such requirements address TCB isolation and non-circumventability of TCB isolation functions.

This threat is also countered through product assurance. The definition of TCB properties assures the consistency of the TCB's behavior. The identification of TCB elements provides the set of elements that determine the protection characteristics of a product. The TCB interface definition establishes the boundary between the TCB and its internal users. Security functional testing establishes that these TCB definitions and properties satisfy the requirements of this Protection Profile, and provide evidence against users being able to bypass the security features of the system.

CS1 Functionality

3. Introduction

This section provides detailed functionality requirements that must be satisfied by an Commercial Security 1 (CS1) compliant product. Note that all plain text are words taken directly from the Federal Criteria [11]. Any assignments or refinements made to the text in the Federal Criteria for this Protection Profile are indicated by the use of ***bold italics***. A Protection Profile requirement is an assignment when it is directly taken as stated from the Federal Criteria component without change or when a binding is made to a Federal Criteria threshold definition. A Protection Profile requirement is a refinement when a Federal Criteria requirement is taken to a lower level of abstraction. The characterization of Protection Profile requirements as being either assignments or refinements can be found at each component level.

This Protection Profile for CS1 utilizes the following levels from the Federal Criteria. Note that not all the components from the Federal Criteria are reflected in this Protection Profile; there are no specific requirements for those components that are not listed.

CS1 Functional Component Summary

Component Name	Component Code	Level
Security Policy Support:		
Identification & Authentication	I&A	1
Audit	AD	1
Access Control	AC	1
Reference Mediation	RM	1
TCB Protection	P	1
Self Checking	SC	1

3.1 Identification & Authentication

All users of the product must be identified and authenticated. A login process is established that the user interacts with in order to provide the information necessary for identification and authentication. The identification and authentication process begins the user's interaction with the target product. First, the user supplies a unique user identifier to the TCB. Then, the user is asked by the TCB to authenticate that claimed identity. The user identifier is used for both access control and also for accountability. Therefore, the proper maintenance and control of the identification mechanism and the identification databases are vital to product security. Once a user has supplied an identifier to the TCB, the TCB must verify that the user really corresponds to the claimed identifier. This is done by the authentication mechanism as described by the following requirements.

For the CS1 level, I&A-1 was assigned from the Federal Criteria. This I&A component level has not been refined from the Federal Criteria.

I&A-1 Minimal Identification and Authentication

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.
2. The TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity.
3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user.

3.2 Audit

Audit supports accountability by providing a trail of user actions. Actions are associated with individual users for security relevant events and are stored in an audit trail. This audit trail can be examined to determine what happened and what user was responsible for a security relevant event. The audit trail data must be protected from unauthorized access, modification, or destruction. In addition, the audit trail data must be available in a useful and timely manner for analysis.

Audit data is recorded from several sources (such as from the TCB or a privileged application) to produce a complete picture of a user's security relevant actions. Therefore, audit data must be correlated across audit collection systems. The mechanisms providing audit data recording must be tailorable to each product's needs. Both the audit data itself and the mechanisms to determine what audit data is recorded are protected by privileges.

Once the audit data is recorded, it is analyzed and reported. At the CS1 level, reports are generated on request.

For the CS1 level, AD-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

AD-1 - Minimal Audit

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

2. The TCB shall be able to record the following types of events:

   - use of the identification and authentication mechanisms;

   - introduction of objects into a user's address space (e.g., file open, program initiation), and deletion of objects;

   - actions taken by computer operators and system administrators and/or system security officers.

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and policy attributes of the object (e.g., object security level).

4. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or object policy attributes (e.g., object security level).

3.3 Access Control

Once the user has been granted access, the question of which objects that authenticated user may access still remains. The requirements below describe these subject accesses to objects.

For the CS1 level, AC-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

AC-1 Minimal Access Control

1. Definition of Access Control Attributes

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined groups or both. Object attributes shall include defined access rights (e.g., read, write, execute) that can be assigned to subject attributes.

2. Administration of Access Control Attributes.

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects. The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users. These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. These controls shall be capable of including or excluding access to the granularity of a single user.

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

The scope of the authorization rules shall include a defined subset of the product's subjects and objects and associated access control attributes. The coverage of authorization rules shall specify the types of objects and subjects to which these rules apply. If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

4. Subject and Object Creation and Destruction

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

3.4 Reference Mediation

Reference mediation, that is, the control by the TCB of subject accesses to objects, must be ensured so that the users can have faith in the TCB's access control decisions. Also, users must be ensured that all access to security services are mediated by the TCB.

For the CS1 level, RM-1 was assigned from the Federal Criteria. No further refinements were made from the Federal Criteria.

RM-1 Mediation of References to a Defined Subject/Object Subset

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.
2. Reference mediation shall include references to the defined subset of subjects, objects, and resources protected under the TCB security policy, and to their policy attributes (e.g., access rights, security and/or integrity levels, role identifiers).
3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

3.5 TCB Protection

TCB protection is a fundamental requirement for a secure product. All of the security components and mechanisms that have been described depend upon the integrity of the TCB and on the TCB being isolated and non-circumventable. The TCB must be resistant to outside penetration.

For the CS1 level, P-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

P-1 Basic TCB Isolation

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains

are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Noncircumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

3.6 TCB Self-Checking

Validating the correct operation of the TCB firmware and hardware is an important aspect of guaranteeing the integrity of the product. Hardware and software features that validate the correct operation of the product will be delivered with the product to ensure that the hardware and firmware are installed properly and are in working order.

For the CS1 level, SC-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

SC-1 Minimal Self Checking

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

CS1 Assurance

4. Introduction

This chapter provides the CS1 development and evaluation assurance requirements package using the development and evaluation assurance components defined in Volume I and the package contained in Volume I, Appendix G of the Federal Criteria. The structure of each assurance package follows that of the assurance components (i.e., each package consists of development process, operational support, development environment, development evidence, and evaluation process components).

Assurance Package T1

This minimal assurance level is intended to include most commercial computer products that incorporate protection components. Minimal assurance refers to the fact that this package includes the lowest levels of development and evaluation assurance components and only those components deemed important to provide the necessary minimal understanding of the product.

The intent of product development assurance for this package is to establish that the external behavior of the product conforms to its user level and administrative documentation without any analysis of the internal structure of the product's TCB. For this reason, only the claimed TCB protection properties, TCB interface description, and TCB element list are required to enable functional testing.

The intent of the operational support assurance for this package is to establish a minimal level of user and administrative guidance and product information that enables the correct product installation, use of product security features, and remediation of flaws.

The development evidence required for this package is commensurate with the assurances required. The intent of this package is to require the type of assurance evidence that is generated during the normal commercial development process.

The intent of evaluation support assurance is to establish that the product, and the context in which it is developed and supported, is commensurate with the development assurance requirements. At the T1 level, testing analysis and the requirement for independent testing determines whether the product minimally meets the functional protection requirements. Operational support evaluation assurance determines whether the product documentation correctly describes the security relevant operations.

The following table summarizes the generic assurance components that comprise the minimal development assurance package (T1):

.

CS1 Assurance Package

Assurance Component Summary	T1
Development Process	
TCB Property Definition	PD-1
TCB Design	
TCB Element Identification	ID-1
TCB Interface Definition	IF-1
TCB Modular Decomposition	----
TCB Structuring Support	----
TCB Design Disciplines	----
TCB Implementation Support	----
TCB Testing & Analysis	
Functional Testing	FT-1
Penetration Analysis	----
Covert Channel Analysis	----
Operational Support	
User's Security Guidance	UG-1
Administrative Guidance	AG-1
Flaw Remediation	----
Trusted Generation	----
Development Environment	
Life Cycle Definition	----
Configuration Management	----
Trusted Distribution	----
Development Evidence	
TCB Protection Properties	EPP-1
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	----
Covert Channel Analysis	----

CS1 Assurance Package

Assurance Component Summary	T1
Product Support	----
Evaluation Process	
Testing	
Test Analysis	TA-1
Independent Testing	IT-1
Review	
Development Environment	---
Operational Support	OSR-1
Analysis	
Protection Properties	---
Design	---
Implementation	---

4.1 TCB Property Definition

The definition of TCB properties assures the consistency of the TCB's behavior. It determines a baseline set of properties that can be used by system developers and evaluators to assure that the TCB satisfies the defined functional requirements.

For CS1, PD-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

PD-1 Property Description

> The developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement.

4.2 TCB Element Identification

The identification of TCB elements (hardware, firmware, software, code, and data structures) provides the set of elements that determine the protection characteristics of a product. All assurance methods rely on the correct identification of TCB elements either directly or indirectly.

For CS1, ID-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

ID-1: TCB Element Identification

> The developer shall identify the TCB elements (i.e., software, hardware/firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).

4.3 TCB Interface Definition

The TCB interface establishes the boundary between the TCB and its external users and application programs. It consists of several components, such as command interfaces (i.e., user oriented devices such as the keyboard and mouse), application program interfaces (system calls), and machine/processor interfaces (processor instructions).

For CS1, IF-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

IF-1: Interface Description

> The developer shall describe all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB. The description shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.
>
> The developer shall identify all call conventions (e.g., parameter order, call sequence requirements) and exceptions signaled at the TCB interface.

4.4 Developer Functional Testing

Functional testing establishes that the TCB interface exhibits the properties necessary to satisfy the requirements of the protection profile. It provides assurance that the TCB satisfies at least its functional protection requirements.

For CS1, FT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

FT-1: Conformance Testing

> The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description.
>
> The developer shall correct all flaws discovered by testing and shall retest the TCB until the protection functions are shown to work as claimed.

4.5 User's Guidance

User's guidance is an operational support assurance component that ensures that usage constraints assumed by the protection profile are understood by the users of the product. It is the primary means available for providing product users with the necessary background and specific information on how to correctly use the product's protection functionality.

For CS1, UG-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

UG-1: Users' Guide

> The developer shall provide a User Guide which describes all protection services provided and enforced by the TCB. The User Guide shall describe the interaction between these services and provide examples of their use. The User Guide may be in the form of a summary, chapter or manual. The User Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

4.6 Administrative Guidance

Administrative guidance is an operation support assurance component that ensures that the environmental constraints assumed by the protection profile are understood by administrative users and operators of the IT product. It is the primary means available to the developer for providing to administrators and operators detailed, accurate information on how to configure and install the product, operate the IT product is a secure manner, make effective use of the product's privileges and protection mechanisms to control access to administrative functions and data bases, and to avoid pitfalls and improper use of the administrative functions that would compromise the TCB and user security.

For CS1, AG-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

AG-1: Basic Administrative Guidance

> The developer shall provide a Trusted Facility Manual intended for the product administrators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB. The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy. The Trusted Facility Manual shall explain the privileges and functions of administrators. The Trusted Facility Manual shall describe the administrative interaction between security services.
>
> The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.

4.7 Evidence of TCB Protection Properties

The documentation of the TCB protection properties includes the definition of the functional component requirements, their modeling (if any), and their interpretation within a product’s TCB. For each requirement of a protection profile, a description, definition (an informal, descriptive specification), or a formal specification of the TCB components and their operation corresponding to the requirement must be provided.

For CS1, EPP-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPP-1 Evidence of TCB Correspondence to the Functional Requirements

> The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. The TCB properties, which are defined by this correspondence, shall be explained in this documentation.

4.8 Evidence of Product Development

Product development evidence consists of the TCB design evidence including the documentation of the TCB interface, TCB elements, TCB structure, TCB structuring support, and TCB design disciplines. The TCB implementation evidence includes TCB source code, and the processor hardware and firmware specifications.

For CS1, EPD-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPD-1: Description Of The TCB External Interface

> The developer shall provide an accurate description of the functions, effects, exceptions and error messages visible at the TCB interface.
>
> The developer shall provide a list of the TCB elements (hardware, software, and firmware).

4.9 Evidence of Functional Testing

Functional testing evidence includes the testing itself, the test plans, and test documentation results. Test plans consist of: the description definition or specification of the test conditions; the test data, which consists of the test environment set-up; the test parameters and expected outcomes; and a description of the test coverage.

For CS1, EFT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EFT-1: Evidence of Conformance Testing

> The developer shall provide evidence of the functional testing that includes the test plan, the test procedures, and the results of the functional testing.

4.10 Test Analysis

Test analysis determines whether the product meets the functional protection requirements defined in the protection profile. Functional testing is based on operational product, the TCB’s functional properties, the product’s operational support guidance, and other producer's documentation as defined by the development evidence requirements. Functional test analysis is based on the achieved test results as compared to the expected results derived from the development evidence.

For CS1, TA-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

TA-1: Elementary Test Analysis

> The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results. The evaluator shall determine whether the product's protection properties, as described in the product documentation have been tested. The evaluator shall assess testing results to determine whether the product's TCB works as claimed.

4.11 Independent Testing

Independent testing determines whether the product's TCB meets the functional protection requirements as defined in the functionality chapter of this Protection Profile. Testing is based on the operational product, the TCB's functional properties, the product's operational support guidance, and other producer's documentation as defined by the Development Evidence requirements.

For CS1, IT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

IT-1: Elementary Independent Testing

> A tester, independent of the producer or evaluator, shall perform functional and elementary penetration testing. This testing shall be based on the product's user and administrative documentation, and on relevant known penetration flaws. Satisfactory completion consists of demonstrating that all user-visible security enforcing functions and security-relevant functions work as described in the product's user and administrative documentation and that no discrepancies exist between the documentation and the product. Test results of the producer shall be confirmed by the results of independent testing. The evaluator may selectively reconfirm any test result.
>
> If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results. The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results. The evaluator shall confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.

COMMERCIAL SECURITY 2 (CS2)

CS2 compliant products provide protection beyond those of the CS1 Protection Profile by providing for the separation of administrative functions and access controls based on groups and access control lists (ACLs). Identification and authentication mechanisms include support for a rigorous password management program (if desired). System entry and availability and recovery requirements are also specified. Secure administrative tools are included, audit mechanisms are expanded, and data reduction tools are listed.

CS2 Functional Component Summary

Component Name	Component Code	Level
Security Policy Support:		
Identification & Authentication	I&A	3
System Entry	SE	2
Trusted Path	TP	1
Audit	AD	3
Access Control	AC	2+
Security Management	SM	2
Reference Mediation	RM	1
TCB Protection	P	1
Self Checking	SC	2
TCB Initialization & Recovery	TR	2
Privileged Operations	PO	1
Ease-of-Use	EU	2

CS2 Assurance Package Summary

Development Assurance Component Summary	T2+
Development Process	
TCB Property Definition	PD-2
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-1
TCB Modular Decomposition	---
TCB Structuring Support	SP-1
TCB Design Disciplines	----

CS2 Assurance Package Summary

Development Assurance Component Summary	T2+
TCB Implementation Support	---
TCB Testing & Analysis	
Functional Testing	FT-1
Penetration Analysis	----
Covert Channel Analysis	----
Operational Support	
User’s Security Guidance	UG-1
Administrative Guidance	AG-1
Flaw Remediation	FR-1
Trusted Generation	TG-2
Development Environment	
Life Cycle Definition	----
Configuration Management	----
Trusted Distribution	---
Development Evidence	
TCB Protection Properties	EPP-2
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	----
Covert Channel Analysis	----
Product Support	EPS-1
Evaluation Process	
Testing	
Test Analysis	TA-1
Independent Testing	IT-1
Review	
Development Environment	----
Operational Support	OSR-1
Analysis	
Protection Properties	---
Design	----
Implementation	---

CS2 Rationale

2.12 Introduction

As outlined in the Federal Criteria, this rationale describes the protection philosophy, how the security features are intended to be used, the assumptions about the environment in which a compliant product is intended to operate, the threats within that environment, and the security features and assurances that counter these threats. At the CS2 level, the features used to counter threats and the strength of the assurance evidence is enhanced over CS1 and is indicated in the text through ***bold italics.***

2.12.1 Protection Philosophy

Any discussion of protection necessarily starts from a protection philosophy, i.e., what it really means to call the product "secure." In general, products will control access to information and other resources through the use of specific security features so that only properly authorized individuals or processes acting on their behalf will be granted access. For CS1, three fundamental requirements are derived for this statement of protection:

- Access authorization
- Accountability
- Assurance

The totality of the functionality that enforces the access authorization and accountability protection philosophy is comprised of the hardware, software, and firmware of the Trusted Computing Base (TCB). CS2 requires the TCB to be ***self-protecting and resistant to bypass*** so that it is effective at countering identified threats. ***CS2 also requires effective management of security attributes and configuration parameters.*** The assurance protection philosophy is comprised of the development process, operational support, development evidence, and evaluation process assurances. Each of these are explained below.

2.12.1.1 Access Authorization

The access authorization portion of the philosophy of protection for this profile addresses subject and object access mediation. For CS2 compliant products, access authorization has been further refined to include system entry, subject and object mediation ***based on Access Control Lists (ACLs), and privileged operations.***

2.12.1.1.1 System Entry

CS2 provides the capability for a system administrator to establish, maintain, and protect information from unauthorized access, and defines the identities of and conditions under which users may gain entry into the system. These system entry controls are based on user identification, time, location, and method of entry.

2.12.1.1.2 Subject and Object Access Mediation

CS2 provides protected access to resources and objects. As defined in the TCSEC and specified in this profile, access control permits system users and the processes that represent them to allow or disallow to other users access to objects under their control:

> Access control is "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject." [1]

These controls permit the granting and revoking of access privileges to be left to the discretion of the individual users. ***The creator of the object becomes, by default, the owner of the object. The owner can grant access as well as specify the mode of access (read, write, execute) to the object.***

ACLs are defined that can effectively specify, for each named object, a list of user identifiers with their respective modes of access (read, write, and execute) to that object. ACLs allow for control of:

- ***objects***
- ***access modes that protect these objects***
- ***specific access permissions to be passed onto identified authorized subjects.***

CS2 also allows for the specification and maintenance of groups. Groups are a convenient means of logically associating user identifiers. Groups can be referenced when specifying ACLs.

2.12.1.1.3 Privileges

CS2 supports and promotes the separation and use of privileges. A privilege enables a subject to perform a security relevant operation that, by default, is denied. Privileges cover all security aspects of a product. CS2 compliant products have tightly controlled privilege definitions as well as control over subjects that hold privileges.

2.12.1.2 Accountability

The accountability portion of the philosophy of protection for this profile addresses user Identification and Authentication (I&A), requirements for security auditing***, and a Trusted Path between a user and the operating system.*** Each of these are explained below.

2.12.1.2.1 Identification and Authentication

User identification is required to support access control and security auditing. This includes the capability to establish, maintain, and protect a unique identifier for each authorized user. User identification is functionally dependent on authentication. Authentication is a method of validating a person as a legitimate user.

User authentication in most computer systems has been provided primarily through the use of passwords. CS2 supports a variety of password features that give the product a great amount of flexibility in the generation of passwords, in password security, password features, and password administration. For most products, a great deal of confidence is placed on maintaining the privacy of passwords belonging to individuals. I&A prevents unauthorized individuals from logging into the product, therefore, password management is essential to secure product operations. The risk of losing a password is addressed within CS2 through promoting the use of stringent password management practices.

In addition, CS2 allows for stronger authentication approaches. CS2 specifies that a unique identifier be associated with each trusted subject such as print spoolers and database management system services. It also requires the TCB to maintain, protect, and display status information for all active users and all enabled or disabled user identities or accounts.

2.12.1.2.2 Audit

For most secure products, a capability must exist to audit the security relevant events. As each user performs security relevant tasks, the product must record the user identifier, the action performed, and the result in a security log. For CS2 compliant products, a capability is specified to allow an system administrator to access and evaluate audit information. This capability provides a method of protection in the sense that security relevant events that occur within a computer system can be logged and the responsible user held accountable for his/her actions. Audit trails are used to detect and deter penetration of a computer system and to reveal activity that identifies misuse.

CS2 provides for an effective audit mechanism by supporting the following basic security characteristics. It provides the ability to:

- review the use of I&A mechanisms;
- discover the introduction of objects into a user's address space;
- discover the deletion of objects;
- discover actions taken by computer operators and system administrators;
- ***audit attempts to violate resource allocation limits;***
- ***protect the audit data so that access to it is limited to system administrators that are authorized to examine audit information;***
- ***discover the use of privileges, such as changing the ownership of an object;***
- ***have the audit mechanism act as a deterrent against penetrators or hackers; and***
- ***use audit reduction tools for assessing the damage that may result in the event of a violation of the implemented security policy. These tools have the capability of selectively reviewing the actions of one or more users or groups, actions performed on a specific object or system resource, and actions associated with specific access control attributes.***

2.12.1.3 Assurance

Assurance addresses all areas of product development assurance and evaluation assurance. Development assurance addresses the development process, operational support, the development environment, and the development evidence. Development process assurance defines the additional efforts that a developer must undertake to satisfy the assurance objectives while creating the product. It specifies how the TCB should be designed and supported by the implementation as well as how it should be tested. Operational support assurance defines the documentation of the security features for both administrative and non-administrative users as well as requirements for TCB flaw

remediation and TCB generation. Development environment assurance includes requirements for defining the product's life cycle and specific features for configuration management. Development evidence assurance defines the TCB's protection properties, details the requirements for product testing and analysis, and defines the requirements for product support. Evaluation assurance establishes that the product, and the context in which it is developed and supported, is commensurate with the development assurance requirements.

The T2+ Assurance Package was chosen for CS2. This package is indicated as being TS2+ since an additional component was included for flaw remediation and for a higher level for trusted generation. This level is intended to include most commercial computer products that are designed to satisfy functional requirements. Although most development assurance components are required at their lowest levels, the requirements of several product development components are extended to capture (1) specific TCB properties, and (2) a rudimentary notion of support for product structure. The operational support component is also extended to enable systematic flaw discovery, tracking, and repair.

The intent of the product development assurance for this package is to establish that the external behavior of the product conforms to its user level and administrative documentation without analysis of the internal structure of the product TCB. For this reason, only the claimed TCB protection properties and their informal models, TCB interface description, and TCB element list are required to enable functional and penetration testing. Support for TCB structuring is limited to process isolation and separation of the protection critical TCB elements from the protection non-critical ones.

The intent of the operational support assurance for this package is to establish a minimal level of user and administrative guidance and product information that enables the correct product installation, use of product security features, and remediation of flaws. Similarly, the development environment assurances are intended to provide a minimal level of control over the product configuration and production. This level of development environment assurance is similar to that already present in most established commercial development organizations.The development evidence required for this package is commensurate with the assurances required. The intent of this package is to require the type of assurance evidence that is generated during the normal commercial development process.

At the T2+ level, evaluation support assurance determines whether the product meets the functional protection requirements for testing analysis and independent testing. Operational support evaluation assurance determines whether the product documentation correctly describes the security relevant operations.

Also for CS2, flaw remediation was included in this assurance package. Flaw remediation is important for commercial environments since it ensures that flaws (i.e, deficiencies in a product that enables a user external to the TCB to violate the functional requirements of a protection profile) that are discovered by the product consumers will be tracked, corrected, and disseminated to the affected customers.

2.12.1.4 Intended Method of Use

All individual users (both administrative and non-administrative users) are assigned a unique user identifier.This user identifier supports individual accountability and access control. The operating system authenticates the claimed identity of the user before allowing the user to perform any further actions.

Products that comply with the CS2 Protection Profile are provided with the capability of assigning privileges to secure functions. These privileges are used to control access to user, password files, and audit trails. This capability is particularly important to prevent a "privileged user" or "superuser" from having a wide set of privileges when only a subset is needed.

A CS1 compliant product imposes controls on authorized users and on processes acting on their behalf to prevent users from gaining access to information and other resources for which they are not authorized. The product provides the capability for users to allow or disallow to other users access to objects under their control. The objects are files that may be read or written to or programs which may be executed. The granularity of control is to the level of individual users (although groups made up of individual users may be specified) and individual objects. CS1 access controls permit the granting and revoking of access to be left to the discretion of the individual users.

Products that comply with CS2 specifications are intended to be used within the following operational constraints:

- The information system is designed to be administered as a unique entity by a single organization.

- The information system is designed to manage computing, storage, input/output, and to control the sharing of resources among multiple users and computer processes.
- The administrative and non-administrative users are identified as distinct individuals.
- The granting and revoking of access control permissions ***(read, write, execute, and deny)*** are left to the discretion of individual users.
- The information system provides facilities for real-time interaction with users that have access to input/output devices.

2.12.2 Environmental Assumptions

A product designed to meet the CS2 Protection Profile is intended to be a general purpose, multi-user operating system that runs on either a workstation, minicomputer, or mainframe. CS2 compliant products are expected to be used in both commercial and government environments. The information being processed may be unclassified, sensitive-but-unclassified, or single-level classified, but not multi-level classified information.

The following specific environmental conditions have been assumed in specifying CS2:

- The product hardware base (e.g., CPU, printers, terminals, etc.), firmware, and software will be protected from unauthorized physical access.
- There will be one or more personnel assigned to manage the product including the security of the information it contains.
- The operational environment will be managed according to the operational environment documentation that is required in the assurance chapter of the Protection Profile.
- The IT product provides a cooperative environment for users to accomplish some task or group of tasks.
- The processing resources of the IT product, including all terminals, are assumed to be located within user spaces that have physical access controls established.
- ***The IT product provides facilities for some or all of the authorized users to create programs that use an Application Programming Interface (API) to enable them to protect themselves and their objects from unauthorized use.***
- ***Fail-safe defaults are included for the access control attributes for the defined subjects and objects for the product.***

2.12.3 Expected Threats

In general, the choice of which Protection Profile to choose depends upon the level of security that is required for that particular organizational environment. The lowest level, the CS1 level, is intended for those commercial and government environments where all the system personnel are trusted and all the data on the system is at the same classification level. For example, a government agency where all personnel has a government clearance, all data is unclassified, and there is no outside network connections would be an ideal candidate for CS1, i.e., the threats to be countered are such that only a minimal level of trust is needed. However, most commercial and government environments are more complex and require a higher degree of trust. CS2 addresses the security needs for the main stream commercial and government environments. It provides a higher level of trust for those organizations that need to enforce a security policy where there is no need for different classifications of data. CS3 is intended to provide the highest level of trust for commercial and government environments. It is intended to be used in those environments where a great deal of trust is required, such as in law enforcement agencies, nuclear facilities, or commercial airports. It provides the strongest features, mechanisms, and assurances to counter these threats.

A product that is designed to meet the CS2 Protection Profile and operate within its assumed environment will provide capabilities to counter these threats. It should be noted, however, that although a product may faithfully implement all the features and assurances specified in this Protection Profile, the complete elimination of any one threat should not be assumed. ***A product that is designed to meet the CS2 Protection Profile is generally known to be more effective at countering the threats than products that meet the CS1 Protection Profile. CS2 products counter all the CS1 threats, and contain stronger features and more assurance evidence than CS1 products. In addition to countering CS1 threats, CS2 compliant products provide protection capabilities to counter four additional threats:***

1. AN UNAUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO THE SYSTEM

For CS1 compliant products, the threat of an unauthorized user gaining access to the system is primarily addressed by I&A. I&A features allow the TCB to verify the identity of individuals attempting to gain access to the system. This is accomplished through the use of passwords.

Although not a direct countermeasure, auditing requirements are specified at the CS1 level to provide the capability to perform an after-the-fact analysis of unauthorized system entry and login attempts. This provides an opportunity for the system administrators to take corrective actions, such as strengthening existing user authentication methods or requiring users to change their passwords.

For CS2 compliant systems, the threat of an unauthorized user gaining access to the system is primarily addressed by stronger I&A features and system entry requirements.

CS2 specifies password requirements that promote a strong organizational password management program. These requirements specify that: null passwords cannot be used during normal operations; passwords be stored in a one-way encrypted form; the clear text representation of a password be automatically suppressed; passwords have a minimum-length; and that the system utilize a password complexity-checking algorithm. An advisory capability is also provided to exclude a list of customer-specified passwords. Such requirements support the use of passwords that are effective against password guessing. To further reduce the probability of a password being guessed, requirements limit the number of attempted login attempts that can be made by a user associated with a specific user identifier. The probability of a single password being guessed is further reduced by requirements for password aging, by having limitations on password reuse, and by allowing users to choose a password that is already associated with another user identifier.

CS2 also allows for a password generating capability. Because random passwords can be difficult to remember and users are tempted to write them down, requirements are specified for the generation of passwords that are easy to remember (i.e., pronounceable). Additionally, an advisory requirement is specified to allow users to choose from a list of alternative passwords.

To minimize the threat that a password has been compromised, a requirement exists to allow a user to change the password. Because a password can be compromised by observing the characters on a terminal screen as it is being typed, there is a requirement to blot out the clear-text representation of the password on the display device.

In addition, requirements are specified to display an advisory warning message to all users prior to system logon to discourage a would-be system penetrator from attempting an unauthorized system entry. Such a message can also provide a basis for subsequent prosecution. System entry requirements also specify additional controls on identified and

authenticated users entering the system. Once a user is authenticated, a check is made to determine if the user is allowed further entry. System entry is granted only in accordance with the authenticated user's access control attributes. These conditions are in terms of a user's identity and his/her membership in groups (if they exist). In addition, CS2 specifies system entry requirements to display to an authorized user, upon successful system entry, the date and time, method of access or port of entry, and the number of failed logon attempts since the last successful system entry by that user identifier. These requirements provide a user with the capability to detect attempted or successful system penetrations. In addition, requirements are specified to lock and terminate an interactive session after an administrator-specified period of user inactivity, and also for the TCB to appear to perform the entire user authentication procedure even if the user identification entered is invalid. The TCB also provides a protected mechanism to allow or deny system entry based on specified ranges of time. Also, conditions for system entry via dial-up lines are required to be specified.

I&A requirements are also enhanced over those of CS1 by specifying requirements for the identification for each trusted user, and by specifying requirements for system administrators to disable a user's identity or account when the number of unsuccessful logon attempts exceeds an administrator specified threshold. This is intended to mitigate the effectiveness of successive attacks of system penetration.

2. AN AUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO RESOURCES WHEN THE USER IS NOT ALLOWED ACCESS

An authorized user can try to gain access to unauthorized resources by assuming the user identifier of another user and thus gaining their associated access rights. This is addressed through the use of passwords.

Once an authorized user has gained access to the system, the threat still remains for a user to gain access to resources when the user is not authorized. At the resource level, CS2 specifies access control features to mediate (i.e., distribute, review, and revoke) user access to a subset of resources.

The object reuse feature has been specified to ensure that resource contents are cleared before they are reused. This reduces the vulnerability that the resource contents can be read before it is overwritten.

To address the vulnerability associated with passwords, CS2 specifies password requirements that promote a strong organizational password management program. Besides those password requirements that address penetration threats from unauthorized users, other password requirements have been specified to counter the threat of an insider (authorized user) attack. There are password requirements that specify that passwords must always be stored in encrypted format and that passwords can never be included in audit trail data. Also, in the event that a user selects a password that is already in use by another user, requirements disallow the system from acknowledging the dual association.

In addition, CS2 specifies access control features to limit the user identifiers that may change to another user identifier that provides any additional privileges to that user. These controls are based on the user identifier and the mode of access (i.e., read, write, and execute). Also, administrators are provided with capabilities through the use of protected mechanisms to set and control security related parameters, defaults, thresholds, attributes, and other security related data. This provides the ability to effectively specify and control access to resources based on site specific protection policies.

CS2 also specifies that privileges must be associated with TCB functions, TCB calls, and accesses to privileged TCB objects (e.g., user and group registration files. password files, audit log files).

CS2 specifies requirements for a direct communication channel, i.e., a trusted path, between the user and the operating system to counter spoofing threats. This security feature provides confidence that a user at a terminal will communicate directly with the TCB rather than to malicious code. In particular, to counter the threat of an authorized user creating a spoof of legitimate user identifier authorization prompts, CS2 specifies requirements for a direct communication path between the user and the authentication system.

Requirements are also specified to display an advisory warning message to all users prior to system logon to discourage unauthorized system entry. Such a message can also provide a basis for subsequent prosecution.

Once an authorized user has been identified and authenticated, system entry control can help counter threats of inadvertent, deliberate, and coerced entry performed in an unauthorized manner by an authorized user. At the end of system entry control, the user

bears the access-control attributes determined during the I&A process, provided that the system entry conditions are satisfied. These conditions can be specified in terms of a user's identity, group membership, or mode of access.

CS2 also provides other security features. Application programming interfaces are provided so that applications can protect themselves and their objects from unauthorized use. CS2 specifies lists of user identities authorized to enter the system via dial-up lines. CS2 also specifies general authentication facilities for use by application developers, system administrators, and users for the protection of resources.

3. SECURITY RELEVANT ACTIONS MAY NOT BE TRACEABLE TO THE USER ASSOCIATED WITH THE EVENT

CS2 accountability and audit requirements are specified to provide the capability to track security relevant actions performed by users, and link such actions, if possible, to the responsible identifier. Audit mechanisms are responsible for the monitoring and detecting of real or potential security violations or events. These audit events can include successful or unsuccessful: I&A events, the introduction of objects into a user's address space, the deletion of objects, and actions taken by system administrators. Each audit record includes the date, time, location, type of event, identity of the user and object involved, and the success or failure of the event.

Requirements are specified to protect audit trail data and the audit control mechanism from unauthorized access, modification, or destruction. Audit features are specified to provide post-collection audit analysis on specific data items, users, and privileged operations. Also, a capability is provided for trusted application programs to append data to the security audit trail.

System entry control helps to enhance accountability by providing a time, space, and mode-of-entry context to each action for which the user is held accountable. These added constraints help to give additional assurance that the proper user is held responsible for a set of authorized actions.

At the CS2 level, tools are specified to enhance the effectiveness of user accountability. CS3 specifies requirements to provide tools to verify the consistency of the audit trial data and the selection of audit events. Tools are also specified for post-collection analysis to selectively review various actions.

4. THE PRODUCT MAY BE DELIVERED, INSTALLED, AND THEN USED IN AN UNSECURED MANNER

This threat is countered by explicitly requiring that the product be delivered with all security features turned on. This ensures that the product is secure by default rather than insecure by default. This is complemented by allowing many security features to be configurable so that, as a specific organization gains experience with the actual threats in its environment, the organization can adjust the degree of security in their system. There are several requirements that reinforce the "security by default" perspective during initial installation. Requirements for security administrative documentation are specified to increase the likelihood that the administrator will install and start the system in a secure manner.

5. SECURITY BREACHES MAY OCCUR BECAUSE AVAILABLE SECURITY FEATURES ARE NOT USED OR ARE USED IMPROPERLY

Requirements for authentication, system and access control, security management, and product documentation provide a basis for countering this threat. Authentication requirements provide for password management procedures to reduce the possibility of easy to guess passwords and to initialize passwords for users. Password generation algorithms are provided that generate easy to remember passwords and that give the user a choice of passwords. In addition, CS2 provides for a capability to import and export objects and subjects with defined access control attributes. This ensures that access control attributes are maintained with the subject or object during import and export operations.

Security management requirements are specified for listing, setting, and updating all of the system security parameters and attributes. These parameters and attributes pertain to identification, authentication, system entry, access control, audit trail analysis and availability features for the system and for individual users. This allows a system administrator to confirm that the system is properly configured and, if necessary, to modify the existing configuration and attributes. In addition, security management requirements provide for routine control and maintenance of system resources.

Product documentation requirements for users and administrators describe how to perform security relevant functions in a secure manner.

6. SECURITY BREACHES MAY OCCUR BECAUSE OF TCB PENETRATION

TCB protection is a fundamental capability of CS compliant products. The security components and mechanisms described in this Protection Profile depend upon the integrity of the TCB and on the TCB being isolated and non-circumventable. CS1 specifies requirements for a common and basic set of security features to protect the TCB from outside penetration.

This threat is also countered through product assurance. The TCB interface definition establishes the boundary between the TCB and its internal users. Security functional testing establishes that these TCB definitions and properties satisfy the requirements of the Protection Profile.

7. USERS MAY BE ABLE TO BYPASS THE SECURITY FEATURES OF THE SYSTEM

This threat is countered by authentication, access control, audit, TCB isolation, TCB non-circumventability, and reference mediation requirements. Authentication requirements protect authentication data from unauthorized users. Resource access control requirements protect access control data.

Audit requirements provide for the logging of successful and unsuccessful accesses to resources as well as for changes made to the system security configuration and system software in the event that the system security features have been bypassed.

CS1 specifications for reference mediation protects the integrity of the access control mechanism and the TCB's functionality. Starting at CS1, requirements exist for TCB mediation of user references to objects and to security relevant services.

CS1-compliant products maintain a domain for its own execution to protect it from external interference and tampering. Such requirements address TCB isolation and non-circumventability of TCB isolation functions.

This threat is also countered through product assurance. The definition of TCB properties assures the consistency of the TCB's behavior. The identification of TCB elements provides the set of elements that determine the protection characteristics of a product. The TCB interface definition establishes the boundary between the TCB and its internal users. Security functional testing establishes that these TCB definitions and properties satisfy the requirements of this Protection Profile, and provide evidence against users being able to bypass the security features of the system. ***At the CS2 level, procedures also have to be es-***

tablished for developers to accept customer reports of protection problems and requests for corrections to those problems. Also, when the product is delivered, all security related parameters must be set to its fail-safe defaults.

8. SUBJECTS MAY BE DENIED CONTINUED ACCESSIBILITY TO THE RESOURCES OF THE SYSTEM (I.E., DENIAL OF SERVICE)

Reliability of service requirements promote the continued accessibility of system resources by authorized subjects. These requirements principally counter threats related to intentional or unintentional denial of service attacks. The requirements include detecting and reporting facilities, controls to limit systematically the disabling of user identifiers, mechanisms for recovery in the event of a system crash, resource quotas, and data backup and restoration. In particular, mechanisms are specified for recovery and system start-up, and for a maintenance mode of operation.

CS2 compliant systems provide the capability to detect and recover from discontinuity of service using some combination of automatic and procedural techniques. This capability is intended to counter the threat that subjects may be denied continued accessibility to the resources of the system (i.e., denial of service). Also, users are notified in advance to change their password, so that access to the system is not denied without warning. An advisory capability exists to allow an system administrator to use null passwords during system start-up. This allows a system administrator to access the system even if the password mechanism has been compromised. In addition, audit trails are compressed to avoid excessive consumption of disk space.

9. THE INTEGRITY OF THE SYSTEM MAY BE COMPROMISED

At the CS2 level, requirements are specified for TCB recovery and start-up to promote the secure state of the system in the event of a system failure or discontinuity of service. These features are intended to minimize the likelihood of the loss of user objects during system recovery.

To protect audit trail data, a mechanism is specified to automatically copy the audit trail file to an alternative storage area.

CS2 compliant products also provide the capability to validate the correct operation of the TCB software, firmware, and hardware. Such features are important to ensure that the software, hardware, and firmware are in working order.

CS2 Functionality

3. Introduction

This section provides detailed functionality requirements that must be satisfied by a Commercial Security 2 (CS2) compliant product. Note that all plain text are words taken directly from the Federal Criteria. Any assignments or refinements made to the text in the Federal Criteria's are indicated by ***bold italics***. A Protection Profile requirement is an assignment when it is directly taken as stated from the Federal Criteria component without change or when a binding is made to a Federal Criteria threshold definition. A Protection Profile requirement is a refinement when the Federal Criteria requirement is taken to a lower level of abstraction. The characterization of Protection Profile requirements as being either assignments or refinements can be found at each component level. Also, note that, unlike the Federal Criteria, there are some items that are considered to be "advisory," i.e., an item marked advisory is a desirable feature but is not required for that component. Each advisory item is marked with an "(A)".

This Protection Profile for CS2 utilizes the following levels from the Federal Criteria. Note that not all the components from the Federal Criteria are reflected in this Protection Profile; there are no specific requirements for those components that are not listed. Also note that a "+" after the component level number indicates that a requirement was included from a higher level of that component.

CS2 Functional Component Summary

Component Name	Component Code	Level
Security Policy Support:		
Identification & Authentication	I&A	3
System Entry	SE	2
Trusted Path	TP	1
Audit	AD	3
Access Control	AC	2+
Security Management	SM	2
Reference Mediation	RM	1
TCB Protection	P	1

CS2 Functional Component Summary

Component Name	Component Code	Level
Self Checking	SC	2
TCB Initialization & Recovery	TR	2
Privileged Operations	PO	1
Ease-of-Use	EU	2

3.1 Identification & Authentication

All users of the product must be identified and authenticated. A login process is established that interacts with the user in order to provide the information necessary for identification and authentication. The identification and authentication process begins the user's interaction with the target product. First, the user supplies a unique user identifier to the TCB. Then, the user is asked to authenticate that claimed identity by the TCB. The user identifier is used for both access control and also for accountability. Therefore, the proper maintenance and control of the identification mechanism and the identification databases are vital to TCB security. Once a user has supplied an identifier to the TCB, the TCB must verify that the user really corresponds to the claimed identifier. This is done by the authentication mechanism as described by the following requirements.

For the CS2 level, I&A-3 was assigned from the Federal Criteria. This I&A component level has been refined from the Federal Criteria by requiring that only system administrators perform certain actions. Password requirements have also been refined to reflect the importance of this protected mechanism to commercial products. An additional refinement was made regarding invalid user identification on error feedback. Assignments were made for default thresholds for the number of login attempts and login time intervals.

I&A-3 Exception-Controlled Identification and Authentication

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2. The TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the product policy attributes of individual users, ***i.e. groups***. These data shall be used by the TCB to authenticate the user's identity and to ensure that the attributes of subjects external to the TCB that may be created to act on behalf of the individual user satisfy the product policy. ***The control of user identification data shall be limited to system administrators, except that a user shall be allowed to modify his/her own authentication data within prescribed limits (e.g., changing his/her own password).***

3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user. The TCB shall appear to perform the entire user authentication procedure even if the user identification entered is invalid. ***Error feedback shall contain no information regarding which part of the authentication information is incorrect.***

The TCB shall end the attempted login session if the user performs the authentication procedure incorrectly for a number of successive times (i.e., a threshold) specified by an authorized system administrator. ***The default threshold shall be three times.*** When the threshold is exceeded, the TCB shall send an alarm message to the system console and/or to the administrator's terminal, log this event in the audit trail, and delay the next login by an interval of time specified by the authorized system administrator. ***The default time interval shall be 60 seconds.*** The TCB shall provide a protected mechanism to disable the user identity or account when the threshold of successive, unsuccessful login attempts is violated more than a number of times specified by the administrator. By default, this mechanism shall be disabled (as it may cause unauthorized denial of service).

4. The TCB shall have the capability to maintain, protect, and display status information for all active users (e.g., users currently logged on, current policy attributes) and of all user accounts (i.e., enabled or disabled user identity or account).

5. Whenever passwords are used as a protection mechanism, then, at a minimum:

a. The TCB shall not indicate to the user if he/she has chosen a password already associated with another user.

b. The TCB shall store passwords in a one-way encrypted form.

  (1) The TCB shall require privilege to access encrypted passwords.

c. The TCB shall automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device.

d. The TCB shall, by default, prohibit the use of null passwords during normal operation.

  (1) A capability, accessible only to an system administrator, to allow null passwords during non-normal operations, such as system start-up, manual recovery, or maintenance mode, on a per-user identifier or per-port basis may be provided. (A)

e. The TCB shall provide a protected mechanism to allow a user to change his or her password. This mechanism shall require re-authentication of the user identity.

- *(1) The TCB shall provide a protected mechanism to set or initialize passwords for users. The use of this mechanism shall be limited to system administrators.*

f. The TCB shall enforce password aging on a per-user identifier or per-group basis (i.e., a user shall be required to change his or her password after a system-specifiable minimum time). The default for all non-system administrators shall be sixty days.

- *(1) The default for system administrator identifiers shall be thirty days.*
- *(2) After the password aging threshold has been reached, the password shall no longer be valid, except as provided in 5 g below.*

The control of password aging shall be limited to system administrators.

g. The TCB shall provide a protected mechanism to notify users in advance of requiring them to change their passwords. This can be done by either:

- *(1) Notifying users a system-specifiable period of time prior to their password expiring. The default shall be seven days.*

- or -

- *(2) Upon password expiration, notifying the user but allowing a system-specifiable subsequent number of additional logons prior to requiring a new password. The default shall be two additional logons.*

The control of user password expiration defaults shall be limited to system administrators.

h. Passwords shall not be reusable by the same user identifier for a system-specifiable period of time. The default shall be six months. The control of password re-use shall be limited to system administrators.

i. The TCB shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:

- *(1) Passwords shall meet a system-specifiable minimum length requirement. The default minimum length shall be eight characters.*
- *(2) The password complexity-checking algorithm shall be modifiable by the TCB. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.*
- *(3) The TCB should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames). (A)*
  - *(a) The TCB should prevent users from selecting a password that matches any of those on the list of excluded passwords. (A)*

The control of password complexity shall be limited to system administrators.

j. If password generation algorithms are present, they shall meet the following requirements:

- *(1) The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable).*

(2) The TCB should give the user a choice of alternative passwords from which to choose. (A)

(3) Passwords shall be reasonably resistant to brute-force password guessing attacks.

(4) If the "alphabet" used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.

(5) The generated sequence of passwords shall have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity).

3.2 System Entry

Once a user is authenticated, a check is made to see if the user is allowed to enter the product. The qualifying checks for system entry at the SE-2 level can include time-of-day, day-of-week, date, location of terminal, or means of access (e.g., dial-up port).

For the CS2 level, SE-2 was assigned from the Federal Criteria. This component has been refined from the Federal Criteria by specifying a default advisory warning to be displayed before user logon, by limiting the control of system entry requirements to system administrators, and by further limiting the use of protected mechanisms to system administrators. Also, default values for terminal locking and session termination and for user policy attributes were assigned.

SE-2 Time and Location Based Entry Control

1. Prior to initiating the system login procedure, the TCB shall display an advisory warning message to the user regarding unauthorized use of the system and the possible consequences of failure to heed this warning.

a. The message shall be system-specifiable.

b. The TCB shall be able to display a message of up to twenty lines in length.

c. The following message shall be displayed by default:

> *"NOTICE: This is a private computer system. All users of this system are subject to having their activities audited. Anyone using this system consents to such auditing. All unauthorized entries or activities revealed by this auditing can be used as evidence and may lead to criminal prosecution."*

The control of system entry messages shall be limited to system administrators.

2. Before system entry is granted to a user, the identity of that user shall be authenticated by the TCB. If the TCB is designed to support multiple login sessions per user identity, the TCB shall provide a protected mechanism to enable limiting the number of login sessions per user identity or account with a default of a single login session. ***The control of this mechanism to limit the number of login sessions shall be limited to system administrators.***

3. The TCB shall grant system entry only in accordance with the authenticated user's policy attributes. The system entry conditions shall be expressed in terms of users' policy attributes***, i.e., user identity and membership to groups.*** If no explicit system-entry conditions are defined, the system-entry default shall be used (e.g., the correct user authentication). The TCB shall provide a protected mechanism to allow or deny system entry based on specified ranges of time. Entry conditions using these ranges shall be specified using time-of-day, day-of-week, and calendar dates. ***The control of system entry conditions shall be limited to system administrators.***

The TCB shall provide a protected mechanism to allow or deny system entry based on location or port of entry. Conditions for system entry via dial-up lines (e.g., lists of user identities authorized to enter the system via dial-up lines), if any, shall be specified.***The control of these mechanisms shall be limited to system administrators***.

4. The TCB shall provide a protected mechanism that enables authorized administrators to display and modify the policy attributes used in system-entry control for each user. The conditions under which an unprivileged user may display these attributes shall be specified.

5. Upon a user's successful entry to the system, the TCB shall display the following data to the user and shall not remove them without user intervention: (1) the date, time, means of access and port of entry of the last successful entry to the system; and (2) the number of successive, unsuccessful attempts to access the system since the last successful entry by the identified user.

6. The TCB shall either lock or terminate an interactive session after an administrator-specified interval of user inactivity. The default value for ***the lock interval shall be five minutes. The default value for session termination shall be fifteen minutes.***

3.3 Trusted Path

A Trusted Path ensures that users have direct, unencumbered communication with the TCB. A Trusted Path may be required at various times during a subject session and also may be initiated by a user during a TCB interaction.

For the CS2 level, TP-1 was assigned from the Federal Criteria. This level was refined by requiring that there be a direct Trusted Path connection to the authentication mechanism.

TP-1 Login Trusted Path

The TCB shall support a trusted communication path between itself and the user for initial identification and authentication. Communications via this path shall be initiated exclusively by a user.

a. ***The TCB shall provide a protected mechanism by which a display device may force a direct connection between the port to which it is connected and the authentication mechanism.***

3.4 Audit

Audit supports accountability by providing a trail of user actions. Actions are associated with individual users for security-relevant events and are stored in an audit trail. This audit trail can be examined to determine what happened and what user was responsible for a security relevant event. The audit trail data must be protected from unauthorized access, modification, or destruction. In addition, the audit trail data must be available in a useful and timely manner for analysis.

Audit data is recorded from several sources (such as the TCB or privileged applications) to produce a complete picture of a user's security relevant actions. Therefore, audit data must be correlated across audit collection systems. The mechanisms providing audit data recording must be tailorable to each product's needs. Both the audit data itself and the mechanisms to determine what audit data is recorded are protected by privileges. Once the audit data is recorded, it is analyzed and reported. At the CS2 level, reporting can be generated on request.

For the CS2 level, AD-4 was assigned from the Federal Criteria. This level was refined from the Federal Criteria by specifying that: password character strings not be recorded in the audit trail; privileged applications be allowed to append data to the audit trail; audit trail files be copied to an alternative storage area after a system-specifiable period of time; the TCB provide a protected mechanism for the automatic deletion of security audit trail files. Assignments were made to subject to object access control rules so that they include user access to disk files, tape volumes, and tape files.

AD-3 Audit Tools

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

The TCB shall support an application program interface that allows a privileged application to append data to the security audit trail or to an applications-specified alternative security audit trail.

The TCB should support an option to maintain the security audit trail data in encrypted format. (A)

2. The TCB shall be able to record the following types of events:

- use of the identification and authentication mechanisms, and system entry events;

- access control events selectable on a per user, per subject, per object, ***per group,*** and/or per policy attribute basis; i.e., introduction of objects into a user's address space (e.g., file open, program initiation), creation and deletion of subjects and objects; distribution and revocation of access rights; changes of subject and object policy attributes; acquisition and deletion of system privileges.

-actions taken by computer operators and system administrators and/or system security officers; i.e., privileged operations such as the modification of TCB elements; accesses to TCB objects ***(at a minimum, access to an object shall include disk file access, tape volume, or tape file access)***; changes of policy attributes of users, TCB configuration and security characteristics, and system privileges; selection and modification of audited events.

The events that are auditable by default, and those that are required for successful auditing of other events, which may not be disabled, shall be defined. The TCB shall provide a protected mechanism that displays the currently selected events and their defaults. The use of this mechanism shall be restricted to authorized system administrators.

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and policy attributes of the object.

The character strings input as a response to a password prompt shall not be recorded in the security audit trail.

4. The TCB shall provide a protected mechanism to turn auditing on and off, and to select and change the events to be audited and their defaults, during the system operation. The use of this mechanism shall be restricted to authorized system administrators. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or object policy attributes. Audit review tools shall be available to authorized system administrators to assist in the inspection and review of audit data, and shall be protected from unauthorized use, modification, or destruction.

The TCB shall provide tools for audit data processing. These shall include specifically designed tools: for verifying the consistency of the audit data; for verifying the selection of audit events; for audit trail management. The audit trail management tools shall enable:

- creation, destruction, and emptying of audit trails; use of warning points regarding the size of the audit data, and modification of the audit trail size;

-formatting and compressing of event records;

-displaying of formatted audit trail data; and

-maintaining the consistency of the audit trail data after system failures and discontinuity of operation.

The TCB shall provide a protected mechanism for the automatic copying of security audit trail files to an alternative storage area after a system-specifiable period of time.

The TCB shall provide a protected mechanism for the automatic deletion of security audit trail files after a system-specifiable period of time. The default shall be thirty days.

(a) It shall not be possible to delete the security audit trail before it gets copied to an alternate storage area.

(b) It shall be possible to disable this mechanism.

The use of audit trail management functions shall be limited to system administrators.

5. Audit review tools shall be available to authorized users to assist in the inspection and review of audit data, and shall be protected from unauthorized modification or destruction. The TCB shall also provide tools for post-collection audit analysis (e.g., intrusion detection) that shall be able to selectively review (1) the actions of one or more users (e.g., identification, authentication, system-entry, and access control actions); (2) the actions performed on a specific object or system resource; and (3) all, or a specified set of, audited exceptions; and (4) actions associated with a specific policy attributes. The review tools shall be able to operate concurrently with the system operation.

3.5 Access Control

Once the user has been granted access, the question of which objects that authenticated user may access still remains. An owner, or an authorized user, allows or denies to other users access to that object. The requirements below describe subject accesses to objects.

For the CS2 level, AC-2+ was assigned from the Federal Criteria. This level is indicated as being AC-2+ because a requirement was included from level AC-4 (the distribution, revocation, and review of access control attributes rules). This is indicated in the text by an

“[AC-4]” in front of the requirement.This component level was refined from the Federal Criteria by specifying: a protected mechanism for groups; a limitation on the changes an active subject can make to a privileged user identifier; a definition of an access control list; and minimum authorization rules.

AC-2+ Basic Access Control

1. Definition of Access Control Attributes

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined groups or both. Object attributes shall include defined access rights (***i.e.,*** read, write, execute) that can be assigned to subject attributes.

The TCB shall be able to assign access rights to group identities.

If multiple access control policies are supported, the access control attributes corresponding to each individual policy shall be identified.

The subject and/or object attributes shall accurately reflect the sensitivity and integrity of the subject or object.

2. Administration of Access Control Attributes

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects.

The TCB shall provide a protected mechanism for groups as follows:

- ***a. A user identifier shall be able to be associated with one or more groups.***
- ***b. The TCB shall provide a protected mechanism to list the names of all groups.***
- ***c. The TCB shall provide a protected mechanism to list the membership of any group.***

Rules for maintaining group membership shall be provided. These rules shall include those for displaying and modifying the list of users belonging to a group and the group attributes of those users.

The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users.

Only the current owner or system administrators shall modify access control attributes on objects.

- ***(a) There should be a distinct access right to modify the contents of an object’s access control list (e.g., an “ownership” or “control” access right). (A)***

The TCB shall provide a protected mechanism to modify group membership. The use of this mechanism shall be under the control of system administrators. Authority to modify specific group membership may be delegated.

The TCB shall provide a protected mechanism by which the user identifier associated with a subject attribute can be changed while the subject is active. It shall also provide a protected mechanism for limiting the user identifiers that may change to a user identifier that would provide any additional access rights. The control of these mechanisms shall be limited to system administrators.

[AC-4]: These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights, ***(i.e., these rules shall define the distribution, revocation, and review of access control attributes)****.* ***The controls defined by these rules shall be capable of specifying for each named object, a list of individuals and a list of groups of named individuals, with their respective access rights to that object. Furthermore, for each named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is given.*** These controls shall be capable of including or excluding access to the granularity of a single user.

The rules for assignment and modification of access control attributes shall include those for attribute assignment to objects during import and export operations. If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

For each object, the authorization rules of the TCB shall be based on a protected mechanism to specify a list of user identifiers or groups with their specific access rights to that object (i.e., an access control list).

At a minimum, the authorization rules shall be defined as follows:

a. ***The access rights associated with a user identifier shall take precedence over the access rights associated with any groups of which that user identifier is a member.***

b. ***When a user identifier can be an active member of multiple groups simultaneously, or if the access rights associated with the user identifier conflict with the access rights associated with any group in which the user is a member, it shall be possible for an system administrator to configure rules that combine the access rights to make a final access control decision.***

c. ***The TCB shall provide a protected mechanism to specify default access rights for user identifiers not otherwise specified either explicitly by a user identifier or implicitly by group membership.***

The scope of the authorization rules shall include a defined subset of the product's subjects and objects and associated access control attributes. The coverage of authorization rules shall specify the types of objects and subjects to which these rules apply. If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

If multiple policies are supported, the authorization rules for each policy shall be defined separately. The TCB shall define and enforce the composition of policies, including the enforcement of the authorization rules (e.g., subject and object type coverage, enforcement precedence).

4. Subject and Object Creation and Destruction

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

3.6 Security Management

The management of security attributes and configuration parameters is an important aspect of a secure product. Mechanisms have to be provided to easily maintain the product, and they must be protected so that only system administrators can manage the security aspects of the product.

For the CS2 level, SM-2 was assigned from the Federal Criteria. This level was refined from the Federal Criteria by specifying that sessions be terminated rather than locked. An assignment was made for the definition and maintenance of groups as a security policy attribute.

SM-2 Basic Security Management

1. The TCB shall provide an installation mechanism for the setting and updating of its configuration parameters, and for the initialization of its protection-relevant data structures before any user or administrator policy attributes are defined. It shall allow the configuration of TCB internal databases and tables.

The TCB shall distinguish between normal mode of operation and maintenance mode, and shall provide a maintenance-mode mechanism for recovery and system start-up.

2. The TCB shall provide protected mechanisms for displaying and modifying the security policy parameters. These parameters shall include identification, authentication, system entry and access control parameters for the entire system and for individual users.

The TCB shall have a capability to define the identification and authentication policy on a system-wide basis (e.g., password minimum and maximum lifetime, password length and complexity parameters). The TCB mechanisms shall have the capability to limit: (1) maximum period of interactive session inactivity, (2) maximum login or session time, and (3) successive unsuccessful attempts to log in to the system. ***In particular, the TCB shall provide a protected mechanism to specify that sessions be terminated rather than locked after a period of inactivity. The control of these mechanisms shall be limited to system administrators.***

3. The TCB shall provide protected mechanisms for manually displaying, modifying, or deleting user registration and account parameters. These parameters shall include unique user identifiers, their account, and their associated user name and affiliation. The TCB shall allow the manual enabling and disabling of user identities and/or accounts.

The TCB shall provide a means to uniquely identify security policy attributes. It shall also provide a means of listing all these attributes for a user, and all the users associated with an attribute. It shall be capable of defining and maintaining the security policy attributes for subjects including: defining and maintaining privileges for privileged subjects, discretionary ***(i.e., definition and maintenance of groups)*** and non-discretionary attributes and centralized distribution, review and revocation of policy attributes.

4. The TCB shall provide protected mechanisms for routine control and maintenance of system resources. It shall allow the enabling and disabling of peripheral devices, mounting of removable storage media, backing-up and recovering user objects; maintaining the TCB hardware and software elements (e.g., on site testing); and starting and shutting down the system.

5. The use of the protected mechanisms for system administration shall be limited to authorized administrative users. ***The control of access-control attributes shall be limited to the object owner and to system administrators.***

3.7 Reference Mediation

Reference mediation, that is, the control by the TCB of subject accesses to objects, must be ensured so that the users can have faith in the TCB's access control decisions. Also, users must be ensured that all access to security services are mediated by the TCB.

For the CS2 level, RM-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

RM-1 Mediation of References to a Defined Subject/Object Subset

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.

2. Reference mediation shall include references to the defined subset of subjects, objects, and resources protected under the TCB security policy, and to their policy attributes (e.g., access rights, security and/or integrity levels, role identifiers).

3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

3.8 Logical TCB Protection

TCB protection is a fundamental requirement for a secure product. All of the security components and mechanisms that have been described depend upon the integrity of the TCB and on the TCB being isolated and non-circumventable. The TCB must be resistant to outside penetration.

For the CS2 level, P-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

P-1 Basic TCB Isolation

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Noncircumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

3.9 TCB Self-Checking

Validating the correct operation of the TCB firmware and hardware is an important aspect of guaranteeing the integrity of the product. Hardware and software features that validate the correct operation of the product will be delivered with the product to ensure that the hardware and firmware are installed properly and are in working order.

For the CS2 level, SC-2 was assigned from the Federal Criteria.The Federal Criteria was refined to limit the execution of operator-controlled tests to system administrators.

SC-2 Basic Self Checking

> Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB. These features shall include: power-on tests, loadable tests, and operator-controlled tests.
>
> The power-on tests shall test all basic components of the TCB hardware and firmware elements including memory boards and memory interconnections; data paths; busses; control logic and processor registers; disk adapters; communication ports; system consoles, and the keyboard speaker. These tests shall cover all components that are necessary to run the loadable tests and the operator-controlled tests.
>
> The loadable tests shall cover: processor components (e.g., arithmetic and logic unit, floating point unit, instruction decode buffers, interrupt controllers, register transfer bus, address translation buffer, cache, and processor-to-memory bus controller); backplane busses; memory controllers; and writable control memory for operator-controlled and remote system-integrity testing.
>
> Operator-controlled tests shall be able to initiate a series of one-time or repeated tests, to log the results of these tests and, if any fault is detected, to direct the integrity-test programs to identify and isolate the failure. ***The execution of operator-controlled tests shall be limited to system administrators.***

3.10 TCB Initialization and Recovery

The recovery and start-up of the TCB must be ensured so that the product always remains in a secure state, whether the recovery is performed manually or automatically.

For the CS2 level, TR-1 was assigned from the Federal Criteria. No further refinements were made from the Federal Criteria.

TR-2 Basic for Recovery or Start-up

1. Procedures and/or mechanisms shall be provided to assure that, after a TCB failure or other discontinuity, recovery without protection compromise is obtained.

2. If automated recovery and start-up is not possible, the TCB shall enter a state where the only system access method is via administrative interfaces, terminals, or procedures. Administrative procedures shall exist to restore the system to a secure state (i.e., a state in which all the security-policy properties hold).

3.11 Privileged Operation

Privileges are associated with functional components so that at any given time only those operations that are associated with the privilege can be performed. The privileges that a product needs must be identified and must cover all the security aspects of the product, including the secure administration of the product, and should be defined so that there is not a single privileged mode for all of the TCB's operations.

For the CS2 level, PO-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

PO-1 Privilege Association with TCB Modules

1. TCB privileges needed by individual functions, or groups of functions, shall be identified. Privileged TCB calls or access to privileged TCB objects, such as user and group registration files, password files, security and integrity-level definition file, role definition file, or audit-log file shall also be identified.

2. The identified privileged functions of a TCB functional component shall be associated only with the privileges necessary to complete their task.

3.12 Ease-of-TCB-Use

If security mechanisms are not easy to use and maintain, then administrative and non-system administrators may be tempted to disable the security mechanisms. Therefore, ease of use becomes an important element in the administration of a secure product and in the creation of privileged applications. It also minimizes errors on the part of both the administrative and non-system administrators, and can serve to minimize the consequences of these errors.

For the CS2 level, EU-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EU-2 Ease of Application Programming

> 1. The TCB shall provide well-defined actions to undertake administrative functions. Default options shall be provided for security parameters of administrative functions.
>
> The TCB shall include fail-safe defaults for the policy attributes of the defined subjects and objects, as well as user-setable defaults for the defined subjects and objects.
>
> 2. The TCB shall provide well-defined application programming interfaces and programming functions (e.g., libraries) for all its policies to support the development of applications that can define and enforce security policies on application-controlled subjects and objects. The TCB shall enable user-controlled reduction of access rights available to applications.

CS2 Assurance

4. Introduction

This chapter provides the CS2 development and evaluation assurance requirements package using the development and evaluation assurance components defined in Volume I and the package contained in Volume I, Appendix G of the Federal Criteria. The structure of each assurance package follows that of the assurance components (i.e., each package consists of development process, operational support, development environment, development evidence, and evaluation process components).

Assurance Package T2+

Assurance package T2+ was chosen for CS2. This package is indicated as being TS2+ since an additional component was included for flaw remediation and a higher level was chosen for trusted generation. This basic assurance level is intended to include most commercial computer products that are designed to satisfy functional requirements. Although most development assurance components are required at their lowest levels, the requirements of several product-development components are extended to capture (1) specific TCB properties, and (2) a rudimentary notion of support for product structure. The operational support component is also extended to enable systematic flaw discovery, tracking, and repair.

The intent of the product development assurance for this package is to establish that the external behavior of the product conforms to its user level and administrative documentation without analysis of the internal structure of the product TCB. For this reason, only the claimed TCB protection properties and their informal models, TCB interface description, and TCB element list are required to enable functional testing. Support for TCB structuring is limited to process isolation and separation of the protection critical TCB elements from the protection non-critical ones.

The intent of the operational support assurance for this package is to establish a minimal level of user and administrative guidance and product information that enables the correct product installation and use of product security features. Similarly, the development environment assurances are intended to provide the a minimal level of control over the product configuration and production. This level of development environment assurance is similar to that already present in most established commercial development organizations.

The development evidence required for this package is commensurate with the assurances required. The intent of this package is to require the type of assurance evidence that is generated during the normal commercial development process.

The intent of evaluation support assurance is to establish that the product, and the context in which it is developed and supported, is commensurate with the development assurance requirements. At the T2+ level, testing analysis and the requirement for independent testing determines whether the product meets the functional protection requirements. Operational support evaluation assurance determines whether the product documentation correctly describes the security relevant operations.

Also for CS2, flaw remediation was included in this package. Flaw remediation is important for commercial environments since it ensures that flaws (i.e, deficiencies in a product that enables a user external to the TCB to violate the functional requirements of a protection profile) that are discovered by the product consumers will be tracked, corrected, and disseminated to the affected customers.

The following table summarizes the generic assurance components that comprise the Basic Development Assurance Package (T2+).

.

CS2 Assurance Package

Development Assurance Component Summary	T2+
Development Process	
TCB Property Definition	PD-2
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-1
TCB Modular Decomposition	----
TCB Structuring Support	SP-1
TCB Design Disciplines	----
TCB Implementation Support	----
TCB Testing & Analysis	

CS2 Assurance Package

Development Assurance Component Summary	T2+
Functional Testing	FT-1
Penetration Analysis	----
Covert Channel Analysis	----
Operational Support	
User's Security Guidance	UG-1
Administrative Guidance	AG-1
Flaw Remediation	FR-1
Trusted Generation	TG-2
Development Environment	
Life Cycle Definition	----
Configuration Management	----
Trusted Distribution	----
Development Evidence	
TCB Protection Properties	EPP-2
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	----
Covert Channel Analysis	----
Product Support	EPS-1
Evaluation Process	
Testing	
Test Analysis	TA-1
Independent Testing	IT-1
Review	
Development Environment	----
Operational Support	OSR-1
Analysis	
Protection Properties	---
Design	----
Implementation	---

4.1 TCB Property Definition

The definition of TCB properties assures the consistency of the TCB's behavior. It determines a baseline set of properties that can be used by system developers and evaluators to assure that the TCB satisfies the defined functional requirements.

For CS2, PD-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

PD-2 Informal Property Identification

> The developer shall provide informal models for the functional components and sub-components of the profile. At a minimum, an informal model of the access control components shall be provided. Each informal model shall include (abstract) data structures and operations defining each functional component or sub-component, and a description of the model properties. The developer shall interpret (e.g., trace) the informal models within the product TCB. For each model entity, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that entity; (2) define the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the model properties. The developer's interpretation of each informal model, which defines the TCB properties, shall identify all TCB elements that do not correspond to any model entity and shall explain why these elements do not render the TCB properties invalid.
>
> For the components that are not informally modeled, the developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement. The developer's interpretation of each functional requirement, which describes the TCB properties, shall identify all TCB elements that do not correspond to any functional requirement and shall explain why these elements do not render the TCB properties invalid.

4.2 TCB Element Identification

The identification of TCB elements (hardware, firmware, software, code, and data structures) provides the set of elements that determine the protection characteristics of a product. All assurance methods rely on the correct identification of TCB elements either directly or indirectly.

For CS2, ID-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

ID-1: TCB Element Identification

> The developer shall identify the TCB elements (i.e., software, hardware/ firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).

4.3 TCB Interface Definition

The TCB interface establishes the boundary between the TCB and its external users and application programs. It consists of several components, such as command interfaces (i.e., user oriented devices such as the keyboard and mouse), application program interfaces (system calls), and machine/processor interfaces (processor instructions).

For CS2, IF-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

IF-1: Interface Description

> The developer shall describe all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB. The description shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.
>
> The developer shall identify all call conventions (e.g., parameter order, call sequence requirements) and exceptions signaled at the TCB interface.

4.4 TCB Structuring Support

Structuring the TCB into modules is necessary. However, the modular decomposition does not necessarily reflect the run-time enforcement of the TCB structuring since the separation of modules may not necessarily be supported by run-time mechanisms. The run-time enforcement of internal TCB structuring adds a measure of assurance that the TCB elements that are critical to the enforcement of the protection functions are separate from the non-critical elements. Also, the use of run-time enforcement of TCB structuring helps separate protection-critical TCB elements from each other, thereby helping to enforce the separation of protection concerns and minimizing the common mechanisms shared between protection critical elements.

For CS3, SP-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

SP-1: Process Isolation

> The TCB shall maintain process isolation.

4.5 Developer Functional Testing

Functional testing establishes that the TCB interface exhibits the properties necessary to satisfy the requirements of the protection profile. It provides assurance that the TCB satisfies at least its functional protection requirements.

For CS2, FT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

FT-1: Conformance Testing

The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description.

The developer shall correct all flaws discovered by testing and shall retest the TCB until the protection functions are shown to work as claimed.

4.6 User’s Guidance

User’s guidance is an operational support assurance component that ensures that usage constraints assumed by the protection profile are understood by the users of the product. It is the primary means available for providing product users with the necessary background and specific information on how to correctly use the product’s protection functionality.

For CS2, UG-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

UG-1: Users' Guide

The developer shall provide a Users' Guide which describes all protection services provided and enforced by the TCB. The User's Guide shall describe the interaction between these services and provide examples of their use. The User's Guide may be in the form of a summary, chapter or manual. The User’s Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

4.7 Administrative Guidance

Administrative guidance is an operation support assurance component that ensures that the environmental constraints assumed by the protection profile are understood by administrative users and operators of the IT product. It is the primary means available to the developer for providing to administrators and operators detailed, accurate information on how to configure and install the product, operate the IT product is a secure manner, make effective use of the product's privileges and protection mechanisms to control access to administrative functions and data bases, and to avoid pitfalls and improper use of the administrative functions that would compromise the TCB and user security.

For CS2, AG-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

AG-1: Basic Administrative Guidance

> The developer shall provide a Trusted Facility Manual intended for the product administrators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB. The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy. The Trusted Facility Manual shall explain the privileges and functions of administrators. The Trusted Facility Manual shall describe the administrative interaction between security services.
>
> The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.

4.8 Flaw Remediation Procedures

Flaw remediation is an operational support assurance component that ensures that flaws (i.e, deficiencies in a product that enables a user external to the TCB to violate the functional requirements of a protection profile) that are discovered by the product consumers will be tracked, corrected, and disseminated to the affected customers.

For CS2, FR-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

FR-1: Basic Flaw Remediation

Flaw Tracking Procedures: The developer shall establish a procedure to track all reported protection flaws in each release of the product. The tracking system shall include a description of the nature and effect of each flaw and the status of finding a correction to the flaw.

Flaw Repair Procedures: The developer shall establish a procedure to identify corrective actions for protection flaws.

Customer Interaction Procedures: The developer shall provide flaw information and corrections to registered customers.

4.9 Trusted Generation

Trusted generation is an operational support assurance component that ensures that the copy of the product's TCB that is configured and activated by the consumer exhibits the same protection properties as the master copy of the product's TCB that was evaluated for compliance with the protection profile. The trusted generation procedures must provide some confidence that the consumer will be aware of what product configuration parameters can affect the protection properties of the TCB. The procedures must encourage the consumer to choose parameter settings that are within the bounds assumed during the product evaluation.

For CS2, TG-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

TG-2: Trusted Generation With Fail-Safe Defaults

The developer shall establish and document the procedures that a customer must perform to generate an operational TCB from the delivered copy of the master TCB. The customer documentation shall identify any system parameters, which are initialized or set during system generation, that affect the TCB's conformance to the protection profile and state the acceptable ranges of values for those parameters. The product shall be delivered with each of these parameters set to its fail-safe defaults.

4.10 Evidence of TCB Protection Properties

The documentation of the TCB protection properties includes the definition of the functional component requirements, their modeling (if any), and their interpretation within a product's TCB. For each requirement of a protection profile, a description, definition (an informal, descriptive specification), or a formal specification of the TCB components and their operation corresponding to the requirement must be provided.

For CS2, EPP-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPP-1 Evidence of TCB Correspondence to the Functional Requirements

> The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. The TCB properties, which are defined by this correspondence, shall be explained in this documentation.

4.11 Evidence of Product Development

Product development evidence consists of the TCB design evidence including the documentation of the TCB interface, TCB elements, TCB structure, TCB structuring support, and TCB design disciplines. The TCB implementation evidence includes TCB source code, and the processor hardware and firmware specifications.

For CS2, EPD-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPD-2: Description Of The TCB External Interface

> The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. The developer shall also provide an informal access control model and its interpretation within the TCB. The TCB properties, which are defined by this correspondence, shall be explained in this documentation.

4.12 Evidence of Functional Testing

Functional testing evidence includes the testing itself, the test plans, and test documentation results. Test plans consist of: the description definition or specification of the test conditions; the test data, which consists of the test environment set-up; the test parameters and expected outcomes; and a description of the test coverage.

For CS2, EFT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EFT-1: Evidence of Conformance Testing

The developer shall provide evidence of the functional testing that includes the test plan, the test procedures and the results of the functional testing.

4.13 Evidence of Product Support

Product support evidence consists of the development environment and operational support documentation and tools. The development environment evidence includes the documentation of the product life-cycle process, configuration management procedures enforced, and the trusted distribution mechanisms and procedures used. It also includes: the identification of the tools used in the product development, configuration management, and trusted distribution; and the characteristics that make those tools suitable for the development of product protection.

For CS2, EPS-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPS-1: Evidence of Basic Product Support

The developer shall provide evidence that describes the policies, procedures, and plans established by the developer to satisfy the Operational Support and Development Environment requirements of the protection profile.

4.14 Test Analysis

Test analysis determines whether the product meets the functional protection requirements defined in the protection profile. Functional testing is based on operational product, the TCB's functional properties, the product's operational support guidance, and other producer's documentation as defined by the development evidence requirements. Functional test analysis is based on the achieved test results as compared to the expected results derived from the development evidence.

For CS2, TA-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

TA-1: Elementary Test Analysis

> The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results. The evaluator shall determine whether the product's protection properties, as described in the product documentation have been tested. The evaluator shall assess testing results to determine whether the product's TCB works as claimed.

4.15 Independent Testing

Independent testing determines whether the product's TCB meets the functional protection requirements as defined in the functionality chapter of this Protection Profile. Testing is based on the operational product, the TCB's functional properties, the product's operational support guidance, and other producer's documentation as defined by the Development Evidence requirements.

For CS2, IT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

IT-1: Elementary Independent Testing

> A tester, independent of the producer or evaluator, shall perform functional and elementary penetration testing. This testing shall be based on the product's user and administrative documentation, and on relevant known penetration flaws. Satisfactory completion consists of demonstrating that

all user-visible security enforcing functions and security-relevant functions work as described in the product's user and administrative documentation and that no discrepancies exist between the documentation and the product. Test results of the producer shall be confirmed by the results of independent testing. The evaluator may selectively reconfirm any test result.

If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results. The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results. The evaluator shall confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.

4.16 Operational Support Review

Operation support review establishes the level of review required to determine whether the product meets the requirements as defined in the protection profile’s Development Assurance subsections for Operational Support including, at the CS2 level, the User and Administrative Guidance documents.

For CS2, OSR-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

OSR-1 Elementary Operational Support Review

The evaluator shall review all documentation focused on the activities of product use (e.g., Users Manuals) and product administration including installation, operation, maintenance, and trusted recovery (e.g., Trusted Facility Management Manuals). This review shall assess the clarity of presentation, difficulty in locating topics of interest, ease of understanding, and completeness of coverage. The need for separate manuals dedicated to protection-relevant aspects of the product should be assessed for effectiveness.

COMMERCIAL SECURITY 3 (CS3)

CS3 compliant products provide enhanced protection beyond those of the CS1 and CS2 Protection Profiles by providing administrative and access control features to centrally control access to information and other resources based on roles. Through the use of role based access controls, a variety of organization specific non-discretionary integrity and confidentiality policies can be specified and enforced. In addition, CS3 provides stronger authentication measures, more administrative tools, and requires a greater degree of assurance evidence.

CS3 Component Summary

Component Name	Component Code	Level
Security Policy Support:		
Identification & Authentication	I&A	4
System Entry	SE	3
Trusted Path	TP	1
Audit	AD	3
Access Control	AC	2+
Availability:		
Resource Allocation	AR	1
Security Management	SM	3
Reference Mediation	RM	1
TCB Protection	P	1
Physical Protection	PP	1
Self Checking	SC	3
TCB Initialization & Recovery	TR	3
Privileged Operations	PO	2
Ease-of-Use	EU	3

CS3 Assurance Package Summary

Assurance Component Summary	T3+
Development Process	
TCB Property Definition	PD-2
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-1
TCB Modular Decomposition	----
TCB Structuring Support	SP-1
TCB Design Disciplines	----
TCB Implementation Support	----
TCB Testing & Analysis	
Functional Testing	FT-1
Penetration Analysis	PA-1
Covert Channel Analysis	----
Operational Support	
User’s Security Guidance	UG-1
Administrative Guidance	AG-2+
Flaw Remediation	FR-2
Trusted Generation	TG-2
Development Environment	
Life Cycle Definition	LC-1
Configuration Management	CM-1
Trusted Distribution	---
Development Evidence	
TCB Protection Properties	EPP-2
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	EPA-1
Covert Channel Analysis	----
Product Support	EPS-1
Evaluation Process	
Testing	
Test Analysis	TA-2
Independent Testing	IT-1
Review	
Development Environment	DER-1
Operational Support	OSR-1
Analysis	
Protection Properties	---
Design	DA-1
Implementation	----

CS3 Rationale

2.17 Introduction

As outlined in the Federal Criteria, this rationale describes the protection philosophy, how the security features are intended to be used, the assumptions about the environment in which a compliant product is intended to operate, the threats within that environment, and the security features and assurances that counter these threats. At the CS3 level, the features used to counter threats and the strength of the assurance evidence is enhanced over CS1 and CS2 and is indicated in the text through ***bold italics.***

2.17.1 Protection Philosophy

Any discussion of protection necessarily starts from a protection philosophy, i.e., what it really means to call the product "secure." In general, products will control access to information and other resources through the use of specific security features so that only properly authorized individuals or processes acting on their behalf will be granted access. For CS1, four fundamental requirements are derived for this statement of protection:

- Access authorization
- Accountability
- Assurance
- ***Availability of Service***

The totality of the functionality that enforces the access authorization and accountability protection philosophy is comprised of the hardware, software, and firmware of the Trusted Computing Base (TCB). CS3 requires the TCB to be self-protecting and resistant to bypass so that it is effective at countering identified threats. CS3 also requires effective management of security attributes and configuration parameters. The assurance protection philosophy is comprised of the development process, operational support, ***development environment,*** development evidence, and evaluation process assurances. Each of these are explained below.

2.17.1.1 Access Authorization

The access authorization portion of the philosophy of protection for this profile addresses subject and object access mediation. For CS3 compliant products, access authorization has been further refined to include system entry, subject and object mediation based on system entry, subject and object mediation ***based on role identifiers***, and privileged operations.

2.17.1.1.1 System Entry

CS3 provides the capability for an system administrator to establish, maintain, and protect information from unauthorized access, and defines the identities of and conditions under which users may gain entry into the system. These system entry controls are based on user identification, ***role*** membership, time, location, and method of entry. ***CS3 strengthens the requirement for locking interactive sessions by requiring the display device to be cleared or overwritten to make the current contents of the screen unreadable.***

2.17.1.1.2 Subject and Object Access Mediation

CS1 and CS2 provide protected access to resources and objects. ***CS3 compliant products also provide the capability of specifying and enforcing access control decisions based on roles [12][13]. In many organizations, the end users do not "own" the information and the programs for which they are allowed access. For these organizations, the corporation or agency is the actual "owner" of the system objects as well as the programs that process them. Control is often based on employee functions rather than on ownership.***

Access control decisions are often determined by the roles individual users take on as part of an organization. The definition of a role includes the specification of duties, responsibilities, and qualifications. For example, the roles an individual associated with a hospital can assume include doctor, nurse, clinician, and pharmacist. Roles in a bank include teller, loan officer, and accountant. Roles can also apply to military systems; for example, target analyst, situation analyst, and traffic analyst are common roles in tactical systems. A Role Based Access Control (RBAC) policy bases access control decisions on the functions a user is allowed to perform within an organization. Under this policy, the users cannot pass access permissions to other users at their discretion.

For each role, a set of transactions associated with the role is maintained. A transaction can be thought of as a transformation procedure [12] (a program or a portion of a program) plus a set of associated data items. In addition, each role has an associated set of individual members.

The determination of membership and the allocation of transactions to a role is in compliance with organization specific non-discretionary policies. These policies can be derived from existing laws, ethics, regulations, or generally accepted practices. These policies are non-discretionary in the sense that they are unavoidably imposed on all users.

For subject and object access mediation, CS3 also provides for additional time and location access control attributes. At a minimum, these attributes include the user's port of entry.

2.17.1.1.3 Privileges

CS3 supports and promotes the separation and use of privileges ***for TCB modules***. A privilege enables a subject to perform a security relevant operation that, by default, is denied. Privileges cover all security aspects of a product, ***including TCB operations performed by system administrators***. CS3 compliant products have tightly controlled privilege definitions as well as control over subjects that hold privileges.

2.17.1.2 Accountability

The accountability portion of the philosophy of protection for this profile addresses user identification and authentication (I&A), requirements for security auditing, and a Trusted Path between a user and the operating system. Each of these are explained below.

2.17.1.2.1 Identification and Authentication

User identification is required to support access control and security auditing. This includes the capability to establish, maintain, and protect a unique identifier for each authorized user. User identification is functionally dependent on authentication. Authentication is a method of validating a person as a legitimate user.

User authentication in most computer systems has been provided primarily through the use of passwords. CS2 supports a variety of password features that give the product a great amount of flexibility in the generation of passwords, in password security, password features, and password administration. For most products, a great deal of confidence is placed on maintaining the privacy of passwords belonging to individuals. I&A prevents unauthorized individuals from logging into the product, therefore, password management is essential to secure product operations. The risk of losing a password is addressed within CS2 through promoting the use of stringent password management practices.

In addition, CS2 allows for stronger authentication approaches. CS2 specifies that a unique identifier be associated with each trusted subject such as print spoolers, database management system services, ***and transaction processing monitors***. It also requires the TCB to maintain, protect, and display status information for all active users and all enabled or disabled user identities or accounts.

CS3 also provides for stronger authentication mechanisms for those commercial and government environments that need such assurance, such as law enforcement agencies, nuclear facilities, and commercial airports. These other approaches can be categorized as "something a user is," which can be indicated through the use of a unique characteristic that a person possesses, or "something a user has," such as a smart card. For example, biometrics is a "something you are" approach for identifying individuals through the use of a unique physical characteristic associated with a person such as a fingerprint or a retina pattern. In many respects, the biometrics approach to user identification is a cleaner and more secure approach than a password mechanism. This method eliminates the concern over the compromise of a password. However, while biometric devices are currently available, their expense makes them impractical for most applications. "Something a user has" requires a physical device that users must have in their possession at authentication time. Usually, these devices require the user to enter a Personal Identification Number (PIN) in case the device is lost or stolen.

2.17.1.2.2 Audit

For most secure products, a capability must exist to audit the security relevant events. As each user performs security relevant tasks, the product must record the user identifier, the action performed, and the result in a security log. For CS31compliant products, a capability is specified to allow a system administrator to access and evaluate audit information. This capability provides a method of protection in the sense that ***all*** security relevant events that occur within a computer system can be logged and the responsible user held accountable for his/her actions. Audit trails are used to detect and deter penetration of a computer system and to reveal activity that identifies misuse.

CS3 provides for an effective audit mechanism by supporting the following basic security characteristics. It provides the ability to:

- review the use of I&A mechanisms;
- discover the introduction of objects into a user's address space;
- discover the deletion of objects;
- discover actions taken by computer operators and system administrators;
- audit attempts to violate resource allocation limits;
- protect the audit data so that access to it is limited to system administrators that are authorized to examine audit information;
- discover the use of privileges, such as changing the ownership of an object;
- have the audit mechanism act as a deterrent against penetrators or hackers; and
- to use audit reduction tools for assessing the damage that may result in the event of a violation of the implemented security policy. These tools have the capability of selectively reviewing the actions of one or more users or ***roles***, actions performed on a specific object or system resource, and actions associated with specific access control attributes.

2.17.1.3 Availability of Service

CS3 promotes the continuous accessibility and usability of resources. The TCB provides the capability to detect and recover from discontinuity of service using some combination of automatic and procedural techniques. Also, resource allocation requirements replace restrictions on the number of subjects and objects a user may have allocated at any given time. This prevents one individual user from denying access to another user's subject and object space.

2.17.1.4 Assurance

Assurance addresses all areas of product development assurance and evaluation assurance. The Development assurance addresses the development process, operational support, the development environment, and the development evidence. Development process assurance defines the additional efforts that a developer must undertake to satisfy the assurance objectives while creating the product. It specifies how the TCB should be designed and supported by the implementation as well as how it should be tested. Operational support assurance defines the documentation of the security features for both administrative and non-administrative users as well as requirements for TCB flaw remediation and TCB generation. Development environment assurance includes requirements for defining the product's life cycle and specific features for configuration management. Development evidence assurance defines the TCB's protection properties, details the requirements for product testing and analysis, and defines the requirements for product support. Evaluation assurance establishes that the product, and the context in which it is developed and supported, is commensurate with the development assurance requirements.

The T3+ Assurance Package was chosen for CS3. This package is indicated as being TS3+ since an additional component was included for flaw remediation. This enhanced assurance level is intended to include the best of the commercial computer products designed to satisfy functional requirements. As such, this package includes several extensions to the assurance components of the previous two packages.

The intent of product development assurance for this package is both to establish that the external behavior of the product conforms to its user level and administrative documentation and to provide visibility into the internal structure of the product's TCB. For this reason, requirements for Descriptive Interface Specifications (DIS) and modular decomposition have been added. TCB element identification and security functional testing have also been extended and penetration testing requirements have been provided to support the added assurances of external behavior.

The intent of the operational support assurance for this package is to establish a level of user and administrative guidance and product information that enables the correct product installation and the use of product security features. The developer is required to establish and document a policy for responding to customer inquiries and flaw remediation. Similarly, the development environment assurances are intended to provide a level of control over the product configuration and production, including well-defined coding standards and strict configuration management processes. This level of development environment assurance is similar to that used in the most advanced commercial development organizations.

The development evidence required for this package is commensurate with the assurances required. The intent of this package is to require the type of assurance evidence that is generated during commercial development oriented towards of high-quality products.

At the T3+ level, evaluation support assurance determines whether the product meets the functional requirements for testing analysis and for independent testing. Operational support evaluation assurance determines whether the product documentation correctly describes the security relevant operations. ***Development environment assurance determines whether the product meets the requirements as defined in the Protection Profile's development assurance subsections. Design assurance determines whether the product meets the design requirements as defined in the Development Process Assurance section of this Protection Profile.***

Also for CS3, flaw remediation was included in this package. Flaw remediation is important for commercial environments since it ensures that flaws (i.e, deficiencies in a product that enables a user external to the TCB to violate the functional requirements of a protection profile) that are discovered by the product consumers will be tracked, corrected, and disseminated to the affected customers. ***Vendors are required to separate protection-relevant fixes from those that are not protection-relevant and must document points of contact for customer error reports.***

2.17.1.5 Intended Method of Use

All individual users (both administrative and non-administrative users) are assigned a unique user identifier. This user identifier supports individual accountability. The operating system authenticates the claimed identity of the user before allowing the user to perform any further actions. ***Upon successful authentication, users are restricted to accessing programs, transactions, and information in a manner that is consistent with their assigned role(s).***

Products that comply with the CS3 Protection Profile are provided with the capability of assigning privileges to ***TCB modules.*** These privileges are used to control access to user and ***role registration files***, password files, and audit trails. Privileges are associated with functional components so that only the privileges necessary to complete a security relevant task can be assigned at a given time. ***Also, privileges are associated with TCB operations performed by system administrators.*** This capability is particularly important to prevent a "privileged user" or "superuser" from having a wide set of privileges when only a subset is needed.

In addition, CS3 provides administrative and access control capabilities that allow for the central administration of a non-discretionary access control policy based on roles. A role specifies a user's set of transactions that allow the user to access resources

through specific functions. Transactions can only be allocated to roles by system administrators. Membership to a role can only be granted and revoked by system administrators.

Products that comply with CS3 specifications are intended to be used within the following operational constraints:

- The information system is designed to be administered as a unique entity by a single organization.
- The information system is designed to manage computing, storage, input/output, and to control the sharing of resources among multiple users and computer processes.
- The administrative and non-administrative users are identified as distinct individuals.
- ***For role based access control, administrators are responsible for interpreting and enforcing organizational policies and protection guidelines that are derived from existing laws, ethics, regulations, or generally accepted practices.***
- The information system provides facilities for real-time interaction with users that have access to input/output devices.
- ***System administrators are selectively assigned privileges that are minimally necessary to perform their security related task.***

2.17.2 Environmental Assumptions

A product designed to meet the CS3 Protection Profile is intended to be a general purpose, multi-user operating system that runs on either a workstation, minicomputer, or mainframe. CS3 compliant products are expected to be used for both commercial and government environments. The information being processed for both commercial and government environments may be unclassified, sensitive-but-unclassified, or single-level classified, but not multi-level classified information.

The following specific environmental conditions have been assumed in specifying CS3:

- The product hardware base (e.g., CPU, printers, terminals, etc.), firmware, and software will be protected from unauthorized physical access.
- There will be one or more personnel assigned to manage the product including the security of the information it contains.

- The operational environment will be managed according to the operational environment documentation that is required in the assurance chapter of the Protection Profile.
- ***Access control to information and other resources is determined by the roles that individual users have.***
- The IT product provides a cooperative environment for users to accomplish some task or group of tasks.
- The processing resources of the IT product, including all terminals, are assumed to be located within user spaces that have physical access controls established.
- The IT product provides facilities for some or all of the authorized users to create programs that use an Application Programming Interface (API) to enable them to protect themselves and their objects from unauthorized use.
- Fail-safe defaults are included for the access control attributes for the defined subjects and objects for the product.

2.17.3 Expected Threats

In general, the choice of which Protection Profile to choose depends upon the level of security that is required for that particular organizational environment. The lowest level, the CS1 level, is intended for those commercial and government environments where all the system personnel are trusted and all the data on the system is at the same classification level. For example, a government agency where all personnel has a government clearance, all data is unclassified, and there is no outside network connections would be an ideal candidate for CS1, i.e., the threats to be countered are such that only a minimal level of trust is needed. However, most commercial and government environments are more complex and require a higher degree of trust. CS2 addresses the security needs for the mainstream commercial and government environments. It provides a higher level of trust for those organizations that need to enforce a security policy where there is no need for different classifications of data. CS3 is intended to provide the highest level of trust for commercial and government environments. It is intended to be used in those environments where a great deal of trust is required, such as in law enforcement agencies, nuclear facilities, or commercial airports. It provides the strongest features, mechanisms, and assurances to counter these threats.

A product that is designed to meet the CS3 Protection Profile and operate within its assumed environment will provide capabilities to counter these threats. It should be noted, however, that although a product may faithfully implement all the features and assurances specified in this Protection Profile, the complete elimination of any one threat should not be assumed. A product that is designed to meet the CS3 Protection Profile is generally known to be more effective at countering the threats than products that meet the CS1 and CS2 Protection Profiles. CS3 products counter all the CS1 and CS2 threats, and contain stronger features and more assurance evidence than CS1 and CS2 products. In addition to countering CS1 and CS2 threats, CS3 compliant products provide protection capabilities to counter one additional threat as follows:

1. AN UNAUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO THE SYSTEM

For CS1 compliant products, the threat of an unauthorized user gaining access to the system is primarily addressed by I&A features that allow the TCB to verify the identity of individuals attempting to gain access to the system. This is accomplished through the use of passwords.

Although not a direct countermeasure, auditing requirements are specified at the CS1 level to provide the capability to perform an after-the-fact analysis of unauthorized system entry and login attempts. This provides an opportunity for the system administrators to take corrective actions, such as strengthening existing user authentication methods or requiring users to change their passwords.

For CS2 compliant systems, the threat of an unauthorized user gaining access to the system is primarily addressed by stronger I&A features and system entry requirements.

CS2 specifies password requirements that promote a strong organizational password management program. These requirements specify that: null passwords cannot be used during normal operations; passwords be stored in a one-way encrypted form; the clear text representation of a password be automatically suppressed; passwords have a minimum-length; and that the system utilize a password complexity-checking algorithm. An advisory capability is also provided to exclude a list of customer-specified passwords. Such requirements support the use of passwords that are effective against password guessing. To further reduce the probability of a password being guessed, requirements limit the number of attempted login attempts that can be made by a user associated with a specific user identifier. The probability of a single password being guessed is further reduced by requirements for password aging, by having limitations on password reuse, and by allowing users to choose a password that is already associated with another user identifier.

CS2 also allows for a password generating capability. Because random passwords can be difficult to remember and users are tempted to write them down, requirements are specified for the generation of passwords that are easy to remember (i.e., pronounceable). Additionally, an advisory requirement is specified to allow users to choose from a list of alternative passwords.

To minimize the threat that a password has been compromised, a requirement exists to allow a user to change the password. Because a password can be compromised by observing the characters on a terminal screen as it is being typed, there is a requirement to blot out the clear-text representation of the password on the display device.

In addition, requirements are specified to display an advisory warning message to all users prior to system logon to discourage a would-be system penetrator from attempting an unauthorized system entry. Such a message can also provide a basis for subsequent prosecution. System entry requirements also specify additional controls on identified and authenticated users entering the system. Once a user is authenticated, a check is made to determine if the user is allowed further entry. System entry is granted only in accordance with the authenticated user's access control attributes. These conditions are in terms of a user's identity and his/her membership in ***roles***. In addition, CS2 specifies system entry requirements to display to an authorized user, upon successful system entry, the date and time, method of access or port of entry, and the number of failed logon attempts since the last successful system entry by that user identifier. These requirements provide a user with the capability to detect attempted or successful system penetrations. In addition, requirements are specified to lock and terminate an interactive session after an administrator-specified period of user inactivity, and also for the TCB to appear to perform the entire user authentication procedure even if the user identification entered is invalid. The TCB also provides a protected mechanism to allow or deny system entry based on specified ranges of time. Also, conditions for system entry via dial-up lines are required to be specified.

I&A requirements are also enhanced over those of CS1 by specifying requirements for the identification for each trusted user, and by specifying requirements for system administrators to disable a user's identity or account when the number of unsuccessful logon attempts exceeds an administrator specified threshold. This is intended to mitigate the effectiveness of successive attacks of system penetration.

Although passwords are currently the most common method for authenticating users, CS3 supports the inclusion of a variety of additional authentication mechanisms, such as smart-cards, cryptographic-based authentication, and biometrics. Also, access

control attributes have been enhanced to include time and location capabilities. This allows an organization to acquire and integrate stronger user authentication capabilities when penetration threats warrant such capabilities.

Also, during system entry, users are granted entry based on their role. In addition, CS3 extends the system entry requirements of CS2 by specifying features for user-initiated locking of the user's interactive sessions (e.g., keyboard locking).

2. AN AUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO RESOURCES WHEN THE USER IS NOT ALLOWED ACCESS

An authorized user can gain access to unauthorized resources by assuming the user identifier of another user and thus gaining their associated access rights. This is addressed through the use of passwords.

Once an authorized user has gained access to the system, the threat still remains for a user to gain access to resources when the uer is not authorized. At the resource level, CS2 specifies access control features to mediate (i.e., distribute, review, and revoke) user access to a subset of resources.

The object reuse feature has been specified to ensure that resource contents are cleared before they are reused. This reduces the vulnerability that the resource contents can be read before it is overwritten.

To address the vulnerability associated with passwords, CS2 specifies password requirements that promote a strong organizational password management program. Besides those password requirements that address penetration threats from unauthorized users, other password requirements have been specified to counter the threat of an insider (authorized user) attack. There are password requirements that specify that passwords must always be stored in encrypted format and that passwords can never be included in audit trail data. Also, in the event that a user selects a password that is already in use by another user, requirements disallow the system from acknowledging the dual association.

In addition, CS3 specifies access control features to limit the ***roles*** that may change to another ***role*** that provides any additional privileges to that user. These controls are based on the ***role*** identifier. Also, administrators are provided with capabilities through the use of protected mechanisms to set and control security related parameters, defaults, thresholds, attributes, and other security related data. This provides the ability to effectively specify and control access to resources based on site specific protection policies.

CS3 also specifies that privileges must be associated with TCB ***modules***, TCB calls, and accesses to privileged TCB objects (e.g., user and ***role*** registration files. password files, audit log files), ***and with TCB operations performed by administrative users.***

CS2 specifies requirements for a direct communication channel, i.e., a trusted path, between the user and the operating system to counter spoofing threats. This security feature provides confidence that a user at a terminal will communicate directly with the TCB rather than to malicious code. In particular, to counter the threat of an authorized user creating a spoof of legitimate user identifier authorization prompts, CS2 specifies requirements for a direct communication path between the user and the authentication system.

Requirements are also specified to display an advisory warning message to all users prior to system logon to discourage unauthorized system entry. Such a message can also provide a basis for subsequent prosecution.

Once an authorized user has been identified and authenticated, system entry control can help counter threats of inadvertent, deliberate, and coerced entry performed in an unauthorized manner by an authorized user. At the end of system entry control, the user bears the access-control attributes determined during the I&A process, provided that the system entry conditions are satisfied. These conditions can be specified in terms of a user's identity, ***role identity***, or mode of access.

CS2 also provides other security features. Application programming interfaces are provided so that applications can protect themselves and their objects from unauthorized use. CS2 specifies lists of user identities authorized to enter the system via dial-up lines. CS2 also specifies general authentication facilities for use by application developers, system administrators, and users for the protection of resources.

To guard against unauthorized user access, CS3 specifies that TCB privileges can be associated with TCB operations performed by system administrators.

Roles are also used as an access control attribute in that access to a particular object may be granted or denied based on a specific role. CS3 also specifies general authentication facilities for use by application developers, system administrators, and users for the enhanced protection of resources. CS3 specifies requirements to provide users with the ability to clear the content of their screens and lock their interactive session without having to logoff the system. This reduces the likelihood that a user will leave his or her terminal while engaged in an active session. Also at the CS3 level, privileges are associ-

ated with TCB operations performed by system administrators. To further strengthen TCB mediation, CS3 expands the scope of authorization rules to include all subject and object contents and all access control attributes.

3. AN AUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO A ROLE WHEN THE USER IS NOT ALLOWED ACCESS

This threat is countered by having a protected mechanism in the TCB that allows only authorized users to access a particular role. Users are prompted for the role they wish to assume for that login session during system entry, and entry will be denied if the user tries to assume a role for which he/she is not authorized. This is assured through security functional testing and through penetration testing. Also, only system administrators are allowed to set role characteristics and to include or delete users from a particular role. Attempts to access and use a particular role can be audited, and the use and definition of roles are explained in security documentation.

4. SECURITY RELEVANT ACTIONS MAY NOT BE TRACEABLE TO THE USER ASSOCIATED WITH THE EVENT

CS3 accountability and audit requirements are specified to provide the capability to track security relevant actions performed by users and link such actions, if possible, to the responsible identifier. Audit mechanisms are responsible for the monitoring and detecting of real or potential security violations or events. These audit events can include successful or unsuccessful: I&A events, the introduction of objects into a user’s address space, the deletion of objects, and actions taken by computer operators and system administrators. Each audit record includes the date, time, location, type of event, identity of the user and object involved, and the success or failure of the event.

Requirements are specified to protect audit trail data and the audit control mechanism from unauthorized access, modification, or destruction. Audit features are specified to provide post-collection audit analysis on specific data items, users, and privileged operations. Also, a capability is provided for trusted application programs to append data to the security audit trail.

System entry control helps to enhance accountability by providing a time, space, and mode-of-entry context to each action for which the user is held accountable. These added constraints help to give additional assurance that the proper user is held responsible for a set of authorized actions.

At the CS2 level, tools are specified to enhance the effectiveness of user accountability. CS3 specifies requirements to provide tools to verify the consistency of the audit trial data and the selection of audit events. Tools are also specified for post-collection analysis to selectively review various actions.

Authentication capabilities are extended to provide for additional authentication methods, for example, tokens or biometrics.

5. THE PRODUCT MAY BE DELIVERED, INSTALLED, AND THEN USED IN AN UNSECURED MANNER

This threat is countered by explicitly requiring that the product be delivered with all security features turned on. This ensures that the product is secure by default rather than insecure by default. This is complemented by allowing many security features to be configurable so that, as a specific organization gains experience with the actual threats in its environment, the organization can adjust the degree of security in their system. There are several requirements that reinforce the “security by default” perspective during initial installation. Requirements for security administrative documentation are specified to increase the likelihood that the administrator will install and start the system in a secure manner.

6. SECURITY BREACHES MAY OCCUR BECAUSE AVAILABLE SECURITY FEATURES ARE NOT USED OR ARE USED IMPROPERLY

Requirements for authentication, system and access control, security management, and product documentation provide a basis for countering this threat. Authentication requirements provide for password management procedures to reduce the possibility of easy to guess passwords and to initialize passwords for users. Password generation algorithms are provided that generate easy to remember passwords and that give the user a choice of passwords. In addition, CS3 provides for a capability to import and export objects and subjects with defined access control attributes. This ensures that access control attributes are maintained with the subject or object during import and export operations.

Security management requirements are specified for listing, setting, and updating all of the system security parameters and attributes. These parameters and attributes pertain to identification, authentication, system entry, access control, audit trail analysis and availability features for the system and for individual users. This allows a system administrator to confirm that the system is properly configured and, if necessary, to modify the existing configuration and attributes. In addition, security management requirements provide for routine control and maintenance of system resources.

Product documentation requirements for users, administrators, ***and operators*** describe how to perform security relevant functions in a secure manner.

CS3 also extends security management requirements with respect to policy-oriented security issues. This includes a means to initialize administrative privileges and administrative identification, authentication, and system entry attributes. Because CS3 compliant systems support multiple I&A methods, the administrator is provided with a capability to specify an authentication method on a per access control attribute basis.

CS3 further extends security management requirements by specifying tools for system administration. These tools include tools for verifying consistency and proper system installation, and for verifying that the TCB does not contain extraneous programs or data.

7. SECURITY BREACHES MAY OCCUR BECAUSE OF TCB PENETRATION

TCB protection is a fundamental capability of CS compliant products. The security components and mechanisms described in this Protection Profile depend upon the integrity of the TCB and on the TCB being isolated and non-circumventable. CS1 specifies requirements for a common and basic set of security features to protect the TCB from outside penetration.

This threat is also countered through product assurance. The TCB interface definition establishes the boundary between the TCB and its internal users. Security functional testing establishes that these TCB definitions and properties satisfy the requirements of this Protection Profile ***and provides evidence against TCB penetration.***

This threat is also countered through penetration testing. The penetration analysis evidence includes, in addition to penetration test plans and results configured in the same manner as the security functional testing evidence, the documentation of the penetration-resistance testing methods and tools, conditions that were verified, the outcomes of the verification and, when appropriate, the scenario of the discovered penetration flaws. Also, the developer must show that all discovered flaws have been eliminated and that no new flaws have been introduced. The cause of every discovered penetration flaw, or class of penetration flaws, must also be documented. At the CS3 level of trust, the sys-

tem developer also must illustrate how, in addition to system reference manuals and TCB interface descriptions, the DIS, source code, and hardware and firmware specifications are used to define penetration test conditions. Also, for each test, the system developer must document all test conditions, data, and coverage.

8. USERS MAY BE ABLE TO BYPASS THE SECURITY FEATURES OF THE SYSTEM

This threat is countered by authentication, access control, audit, TCB isolation, TCB non-circumventability, and reference mediation requirements. Authentication requirements protect authentication data from unauthorized users. Resource access control requirements protect access control data.

Audit requirements provide for the logging of successful and unsuccessful accesses to resources as well as for changes made to the system security configuration and system software in the event that the system security features have been bypassed.

CS1 specifications for reference mediation protects the integrity of the access control mechanism and the TCB's functionality. Starting at CS1, requirements exist for TCB mediation of user references to objects and to security relevant services.

CS1-compliant products maintain a domain for its own execution to protect it from external interference and tampering. Such requirements address TCB isolation and non-circumventability of TCB isolation functions.

This threat is also countered through product assurance. The definition of TCB properties assures the consistency of the TCB's behavior. The identification of TCB elements provides the set of elements that determine the protection characteristics of a product. The TCB interface definition establishes the boundary between the TCB and its internal users. Security functional testing establishes that these TCB definitions and properties satisfy the requirements of the Protection Profile, and provide evidence against subjects being able to bypass the security features of the system. At the CS2 level, procedures also have to be established for developers to accept customer reports of protection problems and requests for corrections to those problems. Also, when the product is delivered, all security related parameters must be set to its fail-safe defaults.

9. SUBJECTS MAY BE DENIED CONTINUED ACCESSIBILITY TO THE RESOURCES OF THE SYSTEM (I.E., DENIAL OF SERVICE)

Reliability of service requirements promote the continued accessibility of system resources by authorized subjects. These requirements principally counter threats related to intentional or unintentional denial of service attacks. The requirements include detecting and reporting facilities, ***features to monitor and control the consumption of disk space and CPU usage***, controls to limit systematically the disabling of user identifiers, mechanisms for recovery in the event of a system crash, resource quotas, destruction of errant processes and facilities for software, and data backup and restoration. In particular, mechanisms are specified for recovery and system start-up, and for a maintenance mode of operation.

CS3 compliant systems provide the capability to detect and recover from discontinuity of service using some combination of automatic and procedural techniques. This capability is intended to counter the threat that subjects may be denied continued accessibility to the resources of the system (i.e., denial of service). Also, users are notified in advance to change their password, so that access to the system is not denied without warning. An advisory capability exists to allow a system administrator to use null passwords during system start-up. This allows a system administrator to access the system even if the password mechanism has been compromised. In addition, audit trails are compressed to avoid excessive consumption of disk space.

CS3 provides the capability to place restrictions on the number of subjects and objects a user may have allocated at any given time. Such capabilities provide protection against a single user denying access to another user's subject and object space. Resource quota requirements are extended to require auditing when attempts are made to violate resource allocation limits.

At the CS3 level, an optional capability can be provided to detect and report conditions that degrade service below a system-specifiable minimum. Also, CS3 provides enhanced TCB checking capabilities by extending TCB checks to not only hardware and firmware but also to software elements (i.e., code and data structures).

10. THE INTEGRITY OF THE SYSTEM MAY BE COMPROMISED

At the CS3 level, requirements are specified for TCB recovery and start-up to promote the secure state of the system in the event of a system failure or discontinuity of service. These features are intended to minimize the likelihood of the loss of user objects during system recovery.

To protect audit trail data, a mechanism is specified to automatically copy the audit trail file to an alternative storage area. ***Also, mechanisms that guarantee the consistency of the audit trail data after system failures and discontinuity of operation is provided.***

CS2 compliant products provide the capability to validate the correct operation of the TCB software, firmware, and hardware. Such features are important to ensure that the software, hardware, and firmware are in working order.

Requirements for the physical security of the TCB and of functions and devices that establish physical control over the TCB are identified and provided. In addition, power-on tests, loadable tests and operator-controlled tests are specified to validate the correct operation of the TCB hardware and firmware.

CS3 also extends the TCB initialization and recovery capabilities by specifying requirements for automatic procedures to protect the secure state of the system in the event of a system failure or discontinuity of service. Also, automated procedures are provided to assure that after system failure or discontinuity of operations a secure state is obtained without undue loss of system or user objects.

CS3 extends the TCB initialization and recovery capabilities by specifying automated procedures to assure that after system failure, other discontinuity, or start-up, a secure state is obtained without undue loss of system or user objects.

At the CS3 level, tools are specified to verify the consistency of audit data and also to check for storage medium and file system integrity. An optional capability is provided to allow for the encryption of data to preserve the integrity of data in an object.

In addition, fail-safe defaults are specified for the access control attributes of subjects, objects, and services used in common system configurations.

CS3 Functionality

3. Introduction

This section provides detailed functionality requirements that must be satisfied by an Commercial Security 3 (CS3) compliant product. Note that all plain text are words taken directly from CS2 's functionality chapter for the components or, for those components not included in CS2, directly from the Federal Criteria. Any assignments or refinements that were made at CS2 are indicated by *italics.* Any assignments or refinements made to the text in CS2 or the Federal Criteria are indicated by ***bold italics.*** A Protection Profile requirement is an assignment when it is directly taken as stated from the component without change or when a binding is made to a Federal Criteria threshold definition. A Protection Profile requirement is a refinement when the requirement is taken to a lower level of abstraction.The characterization of Protection Profile requirements as being either assignments or refinements can be found at each component level. Also, note that, unlike the Federal Criteria, there are some items that are considered to be "advisory," i.e.,an item marked advisory is a desirable feature but is not required for that component. Each advisory item is marked with an "(A)".

This Protection Profile for CS3 utilizes the following levels from the Federal Criteria. Note that not all the components from the Federal Criteria are reflected in this Protection Profile; there are no specific requirements for those components that are not listed. Also note that a "+" after the component level number indicates that a requirement was included from a higher level of that component.

CS3 Functional Component Summary

Component Name	Component Code	Level
Security Policy Support:		
Identification & Authentication	I&A	4
System Entry	SE	3
Trusted Path	TP	1
Audit	AD	3
Access Control	AC	2+
Availability:		

CS3 Functional Component Summary

Component Name	Component Code	Level
Resource Allocation	AR	1
Security Management	SM	3
Reference Mediation	RM	1
TCB Protection	P	1
Physical Protection	PP	1
Self Checking	SC	3
TCB Initialization & Recovery	TR	3
Privileged Operations	PO	2
Ease-of-Use	EU	3

3.1 Identification & Authentication

All users of the product must be identified and authenticated. A login process is established that interacts with the user in order to provide the information necessary for identification and authentication. The identification and authentication process begins the user's interaction with the target product. First, the user supplies a unique user identifier to the TCB. Then, the user is asked to authenticate that claimed identity by the TCB. The user identifier is used for accountability. Therefore, the proper maintenance and control of the identification mechanism and the identification databases are vital to TCB security. Once a user has supplied an identifier to the TCB, the TCB must verify that the user really corresponds to the claimed identifier. This is done by the authentication mechanism as described by the following requirements.

For the CS3 level, I&A-4 was assigned from the Federal Criteria. Refinements were made from CS2 and the Federal Criteria to limit the enforcement of separate user authentication procedures to system administrators.

I&A-4 Exception-Controlled Identification and Authentication

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual. Furthermore, the TCB shall have the capability of associating a unique identity with each privileged subject, ***i.e. transaction processing monitors.***

2. The TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords), as well as information for determining the product policy attributes of individual users, ***i.e. roles***. These data shall be used by the TCB to authenticate the user's identity and to ensure that the attributes of subjects external to the TCB that may be created to act on behalf of the individual user satisfy the product policy. *The control of user identification data shall be limited to system administrators, except that a user shall be allowed to modify his/her own authentication data within prescribed limits (e.g., changing his/her own password).*

The TCB shall be able to incorporate and use installable authentication mechanisms, such as token-based cards, biometrics, or trusted third-party mechanisms, in the place of or in addition to the default authentication (e.g., password-based) mechanism, to authenticate the user. The TCB shall be able to enforce separate user authentication procedures based on specific policy attributes. ***The enforcement of separate user authentication procedures shall be limited to system administrators.***

3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user. The TCB shall appear to perform the entire user authentication procedure even if the user identification entered is invalid. *Error feedback shall contain no information regarding which part of the authentication information is incorrect.*

The TCB shall end the attempted login session if the user performs the authentication procedure incorrectly for a number of successive times (i.e., a threshold) specified by an authorized system administrator. *The default threshold shall be three times.* When the threshold is exceeded, the TCB shall send an alarm message to the system console and/or to the administrator's terminal, log this event in the audit trail, and delay the next login by an interval of time specified by the authorized system administrator. *The default time interval shall be 60 seconds.* The TCB shall provide a protected mechanism to disable the user identity or account when the threshold of successive, unsuccessful login attempts is violated more than a number of times specified by the administrator. By default, this mechanism shall be disabled (as it may cause unauthorized denial of service).

4. The TCB shall have the capability to maintain, protect, and display status information for all active users (e.g., users currently logged on, current policy attributes) and of all user accounts (i.e., enabled or disabled user identity or account).

5. Whenever passwords are used as a protection mechanism, then, at a minimum:

a. The TCB shall not indicate to the user if he/she has chosen a password already associated with another user.

b. The TCB shall store passwords in a one-way encrypted form.

(1) The TCB shall require privilege to access encrypted passwords.

c. The TCB shall automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device.

d. The TCB shall, by default, prohibit the use of null passwords during normal operation.

(1) A capability, accessible only to an system administrator, to allow null passwords during non-normal operations, such as system start-up, manual recovery, or maintenance mode, on a per-user identifier or per-port basis may be provided. (A)

e. The TCB shall provide a protected mechanism to allow a user to change his or her password. This mechanism shall require re-authentication of the user identity.

(1) The TCB shall provide a protected mechanism to set or initialize passwords for users. The use of this mechanism shall be limited to system administrators.

f. The TCB shall enforce password aging on a per-user identifier or per-group basis (i.e., a user shall be required to change his or her password after a system-specifiable minimum time). The default for all non-system administrators shall be sixty days.

(1) The default for system administrator identifiers shall be thirty days.

(2) After the password aging threshold has been reached, the password shall no longer be valid, except as provided in 5 g below.

The control of password aging shall be limited to system administrators.

g. The TCB shall provide a protected mechanism to notify users in advance of requiring them to change their passwords. This can be done by either:

(1) Notifying users a system-specifiable period of time prior to their password expiring. The default shall be seven days.

- or -

(2) Upon password expiration, notifying the user but allowing a system-specifiable subsequent number of additional logons prior to requiring a new password. The default shall be two additional logons.

The control of user password expiration defaults shall be limited to system administrators.

h. Passwords shall not be reusable by the same user identifier for a system-specifiable period of time. The default shall be six months. The control of password re-use shall be limited to system administrators.

i. The TCB shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:

(1) Passwords shall meet a system-specifiable minimum length requirement. The default minimum length shall be eight characters.

(2) The password complexity-checking algorithm shall be modifiable by the TCB. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.

(3) The TCB should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames). (A)

(a) The TCB should prevent users from selecting a password that matches any of those on the list of excluded passwords. (A)

The control of password complexity shall be limited to system administrators.

j. If password generation algorithms are present, they shall meet the following requirements:
  - *(1) The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable).*
  - *(2) The TCB should give the user a choice of alternative passwords from which to choose. (A)*
  - *(3) Passwords shall be reasonably resistant to brute-force password guessing attacks.*
  - *(4) If the "alphabet" used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.*
  - *(5) The generated sequence of passwords shall have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity).*

3.2 System Entry

Once a user is authenticated, a check is made to see if the user is allowed to access the product. The qualifying checks for system entry can include time-of-day, day-of-week, date, location of terminal, or means of access (e.g., dial-up port), and membership in roles.

For the CS3 level, SE-3 was assigned from the Federal Criteria. An assignment was made from CS2 or the Federal Criteria for specifying a role as a user policy attribute.

SE-3 Session Locking and Unlocking

1. Prior to initiating the system login procedure, the TCB shall display an advisory warning message to the user regarding unauthorized use of the system and the possible consequences of failure to heed this warning.

a. The message shall be system-specifiable.

b. The TCB shall be able to display a message of up to twenty lines in length.

c. The following message shall be displayed by default:

> *"NOTICE: This is a private computer system. All users of this system are subject to having their activities audited. Anyone using this system consents to such auditing. All unauthorized entries or activities revealed by this auditing can be used as evidence and may lead to criminal prosecution."*

The control of system entry messages shall be limited to system administrators.

2. Before system entry is granted to a user, the identity of that user shall be authenticated by the TCB. If the TCB is designed to support multiple login sessions per user identity, the TCB shall provide a protected mechanism to enable limiting the number of login sessions per user identity or account with a default of a single login session. *The control of this mechanism to limit the number of login sessions shall be limited to system administrators.*

3. The TCB shall grant system entry only in accordance with the authenticated user's policy attributes. The system entry conditions shall be expressed in terms of users' policy attributes***, i.e., user identity and membership to roles.*** If no explicit system-entry conditions are defined, the system-entry default shall be used (e.g., the correct user authentication). The TCB shall provide a protected mechanism to allow or deny system entry based on specified ranges of time. Entry conditions using these ranges shall be specified using time-of-day, day-of-week, and calendar dates. *The control of system entry conditions shall be limited to system administrators.*

The TCB shall provide a protected mechanism to allow or deny system entry based on location or port of entry. Conditions for system entry via dial-up lines (e.g., lists of user identities authorized to enter the system via dial-up lines), if any, shall be specified.*The control of these mechanisms shall be limited to system administrators.*

4. The TCB shall provide a protected mechanism that enables authorized administrators to display and modify the policy attributes used in system-entry control for each user. The conditions under which an unprivileged user may display these attributes shall be specified.

5. Upon a user's successful entry to the system, the TCB shall display the following data to the user and shall not remove them without user intervention: (1) the date, time, means of access and port of entry of the last successful entry to the system; and (2) the number of successive, unsuccessful attempts to access the system since the last successful entry by the identified user.

6. The TCB shall either lock or terminate an interactive session after an administrator-specified interval of user inactivity. The default value for *the lock interval shall be five minutes. The default value for session termination shall be fifteen minutes.* The TCB shall also provide a mechanism for user-initiated locking of the user's own interactive sessions (e.g., keyboard locking) that includes: (1) clearing or over-writing display devices to make the current contents unreadable; (2) requiring user authentication prior to unlocking the session; and (3) disabling any activity of the user's data entry/display devices other than unlocking the session.

3.3 Trusted Path

A Trusted Path ensures that users have direct, unencumbered communication with the TCB. A Trusted Path may be required at various times during a subject session and also may be initiated by a user during a TCB interaction.

For the CS3 level, TP-1 was assigned from the Federal Criteria. There are no refinements from CS2 or the Federal Criteria.

TP-1 Login Trusted Path

The TCB shall support a trusted communication path between itself and the user for initial identification and authentication. Communications via this path shall be initiated exclusively by a user.

a. The TCB shall provide a protected mechanism by which a display device may force a direct connection between the port to which it is connected and the authentication mechanism.

3.4 Audit

Audit supports accountability by providing a trail of user actions. Actions are associated with individual users for security-relevant events and are stored in an audit trail. This audit trail can be examined to determine what happened and what user was responsible for a security relevant event. The audit trail data must be protected from unauthorized access, modification, or destruction. In addition, the audit trail data must be available in a useful and timely manner for analysis.

Audit data is recorded from several sources (such as the TCB or privileged applications) to produce a complete picture of a user's security relevant actions. Therefore, audit data must be correlated across audit collection systems. The mechanisms providing audit data recording must be tailorable to each product's needs. Both the audit data itself and the mechanisms to determine what audit data is recorded are protected by privileges. Once the audit data is recorded, it is analyzed and reported. Reporting can be by reports generated on request.

For the CS3 level, AD-3 was assigned from the Federal Criteria. A refinement was made to audit attempts to circumvent or gain unauthorized access to resource allocation limits.

AD-3 Audit Tools

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

The TCB shall support an application program interface that allows a privileged application to append data to the security audit trail or to an applications-specified alternative security audit trail.

The TCB should support an option to maintain the security audit trail data in encrypted format. (A)

2. The TCB shall be able to record the following types of events:

- use of the identification and authentication mechanisms, and system entry events;

- access control events selectable on a per user, per subject, per object, ***per role,*** and/or per policy attribute basis; i.e., introduction of objects into a user's address space (e.g., file open, program initiation), creation and deletion of subjects and objects; distribution and revocation of access rights; changes of subject and object policy attributes; acquisition and deletion of system privileges.

-actions taken by computer operators and system administrators and/or system security officers; i.e., privileged operations such as the modification of TCB elements; accesses to TCB objects *(at a minimum, access to an object shall include disk file access, tape volume, or tape file access);* changes of policy attributes of users, TCB configuration and security characteristics, and system privileges; selection and modification of audited events.

- attempts to circumvent or otherwise gain unauthorized access to resource allocation limits.

The events that are auditable by default, and those that are required for successful auditing of other events, which may not be disabled, shall be defined. The TCB shall provide a protected mechanism that displays the currently selected events and their defaults. The use of this mechanism shall be restricted to authorized system administrators.

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and policy attributes of the object.

The character strings input as a response to a password prompt shall not be recorded in the security audit trail.

4. The TCB shall provide a protected mechanism to turn auditing on and off, and to select and change the events to be audited and their defaults, during the system operation. The use of this mechanism shall be restricted to authorized system administrators. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or object policy attributes. Audit review tools shall be available to authorized system administrators to assist in the inspection and review of audit data, and shall be protected from unauthorized use, modification, or destruction.

The TCB shall provide tools for audit data processing. These shall include specifically designed tools: for verifying the consistency of the audit data; for verifying the selection of audit events; for audit trail management. The audit trail management tools shall enable:

- creation, destruction, and emptying of audit trails; use of warning points regarding the size of the audit data, and modification of the audit trail size;

-formatting and compressing of event records;

-displaying of formatted audit trail data; and

-maintaining the consistency of the audit trail data after system failures and discontinuity of operation.

The TCB shall provide a protected mechanism for the automatic copying of security audit trail files to an alternative storage area after a system-specifiable period of time.

The TCB shall provide a protected mechanism for the automatic deletion of security audit trail files after a system-specifiable period of time. The default shall be thirty days.

(a) It shall not be possible to delete the security audit trail before it gets copied to an alternate storage area.

(b) It shall be possible to disable this mechanism.

The use of audit trail management functions shall be limited to system administrators.

5. Audit review tools shall be available to authorized users to assist in the inspection and review of audit data, and shall be protected from unauthorized modification or destruction. The TCB shall also provide tools for post-collection audit analysis (e.g., intrusion detection) that shall be able to selectively review (1) the actions of one or more users (e.g., identification, authentication, system-entry, and access control actions); (2) the actions performed on a specific object or system resource; and (3) all, or a specified set of, audited exceptions; and (4) actions associated with a specific policyattributes.The review tools shall be able to operate concurrently with the system operation.

3.5 Access Control

Once the user has been granted access, the question of which objects the authenticated user may access still remains. An owner, or an authorized user, allows or denies to other users access to that object. The requirements below describe subject accesses to objects.

For the CS3 level, AC-2+ was assigned from the Federal Criteria.his level is indicated as being AC-2+ because requirements were included from level AC-4 (to include the requirements for time and location dependency conditions). These are indicated in the text by an "[AC-4]" in front of the requirement. This component level was refined from CS2 and the Federal Criteria by specifying access control decisions based on roles.

AC-2+ Basic Access Control

1. **Definition of Access Control Attributes**

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined ***roles*** or both. Object attributes shall include defined access rights (*i.e.*, read, write, execute) that can be assigned to subject attributes.

The TCB shall be able to assign access rights to ***role*** *identities.*

If multiple access control policies are supported, the access control attributes corresponding to each individual policy shall be identified.

[AC-4]: The subject and object attributes shall accurately reflect the sensitivity and/or integrity of the subject or object.***The subject's access control attributes also shall include time and location attributes that can be assigned to authenticated user identities.***

2. **Administration of Access Control Attributes**

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects.

The TCB shall provide a protected mechanism for **roles** *as follows:*

a. *A user identifier shall be able to be associated with one or more* **roles.**
b. *The TCB shall provide a protected mechanism to list the names of all* ***roles***.
c. *The TCB shall provide a protected mechanism to list the membership of any* ***role***.

Rules for maintaining **role** *membership shall be provided. These rules shall include those for displaying and modifying the list of users belonging to a* ***role*** *and the* ***role*** *attributes of those users.*

The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users.

Only the current owner or system administrators shall modify access control attributes on objects.

The TCB shall provide a protected mechanism to modify **role** *membership. The use of this mechanism shall be under the control of system administrators. Authority to modify specific* **role** *membership may be delegated.*

The TCB shall provide a protected mechanism by which the user identifier associated with a subject attribute can be changed while the subject is *active. It shall also provide a protected mechanism for limiting the user identifiers that may change to a user identifier that would provide any additional access rights. The control of these mechanisms shall be limited to system administrators.*

[AC-4]: These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined ***roles*** of individuals, or by both, and shall provide controls to limit propagation of access rights, *(i.e., these rules shall define the distribution, revocation, and review of access control attributes). The controls defined by these rules shall be capable of specifying for each named object, a list of individuals and a list of* **roles** *of named individuals, with their respective access rights to that object. Furthermore, for each named object, it shall be possible to specify a list of named individuals and a list of* **roles** *of named individuals for which no access to the object is given.* These controls shall be capable of including or excluding access to the granularity of a single user.***These controls shall also be capable of specifying access-time dependency (i.e., the effect of the distribution and revocation of access control attributes take place at a certain time and shall last for a specified period of time), and/or access-location dependency (i.e., shall specify the locations from which the distribution and revocation of access rights shall take place).***

The rules for assignment and modification of access control attributes shall include those for attribute assignment to objects during import and export operations. If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

[AC-4]: The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. ***These rules shall include time-of-access and location-of-access controls defined for subjects and objects.***

For each object, the authorization rules of the TCB shall be based on a protected mechanism to specify **roles** *with their specific access rights to that object.*
The authorization rules shall be defined in terms of subject authorization conditions for accessing the object (i.e., on <subject, action, object> tuples.

At a minimum, the authorization rules shall be defined as follows:

a. *The access rights associated with a user identifier shall take precedence over the access rights associated with any* **roles** *of which that user identifier is a member.*
b. *When a user identifier can be an active member of multiple* **roles** *simultaneously, or if the access rights associated with the user identifier conflict with the access rights associated with any* **role** *in which the user is a member, it shall be possible for an system administrator to configure*

rules that combine the access rights to make a final access control decision.

c. *The TCB shall provide a protected mechanism to specify default access rights for user identifiers not otherwise specified either explicitly by a user identifier or implicitly by* ***role*** *membership.*

The scope of the authorization rules shall include a defined subset of the product's subjects and objects and associated access control attributes. The coverage of authorization rules shall specify the types of objects and subjects to which these rules apply. If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

If multiple policies are supported, the authorization rules for each policy shall be defined separately. The TCB shall define and enforce the composition of policies, including the enforcement of the authorization rules (e.g., subject and object type coverage, enforcement precedence).

4. **Subject and Object Creation and Destruction**

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

3.6 Security Management

The management of security attributes and configuration parameters is an important aspect of a secure product. Mechanisms have to be provided to easily maintain the product, and they must be protected so that only system administrators can manage the security aspects of the product.

For the CS3 level, SM-2 was assigned from the Federal Criteria. An assignment was made to this component from the Federal Criteria to limit the number of login sessions and for controlling the availability of system resources. A refinement was made to provide system administrators with a protected mechanism for grating and revoking role membership.

SM-3 Policy-Oriented Security Management

1. The TCB shall provide an installation mechanism for the setting and updating of its configuration parameters, and for the initialization of its protection-relevant data structures before any user or administrator policy attributes are defined. It shall allow the configuration of TCB internal databases and tables.

The TCB shall distinguish between normal mode of operation and maintenance mode, and shall provide a maintenance-mode mechanism for recovery and system start-up.This mechanism shall include a means to initialize administrative privileges and administrative identification, authentication, and system-entry attributes.

2. The TCB shall provide protected mechanisms for displaying and modifying the security policy parameters. These parameters shall include identification, authentication, system entry and access control parameters for the entire system and for individual users.

The TCB shall have a capability to define the identification and authentication policy on a system-wide basis (e.g., password minimum and maximum lifetime, password length and complexity parameters). The TCB mechanisms shall have the capability to limit: (1) maximum period of interactive session inactivity, (2) maximum login or session time, and (3) successive unsuccessful attempts to log in to the system. *In particular, the TCB shall provide a protected mechanism to specify that sessions be terminated rather than locked after a period of inactivity.* The control of these mechanisms shall be limited to system administrators.The TCB shall provide an administrative capability to specify the authentication method on a per policy-attribute basis whenever multiple identification and authentication methods are used; e.g., via user passwords, tokens, or biometrics.

If the TCB is designed to support multiple login sessions per user identity, the administrators shall be able to limit the number of simultaneous login sessions on an authorization-attribute basis. ***The system-supplied default shall limit each user identifier to one simultaneous logon session.***

The TCB shall also have a capability to limit the successive unsuccessful attempts to login from a specific port of entry, and/or with a specific user identity or account.

The TCB shall provide a mechanism to control the availability of system resources via resource quotas and quantity-of-resources limits.

3. The TCB shall provide protected mechanisms for manually displaying, modifying, or deleting user registration and account parameters. These parameters shall include unique user identifiers, their account, and their associated user name and affiliation. The TCB shall allow the automatic disabling of user identities and/ or accounts, after a period during which the identity and/or account have not been used. The time period shall be administrator specified, with a specified default provided. The TCB shall allow the automatic re-enabling of disabled user identities and/or accounts after an administrator-specified period of time.

The TCB shall provide a means to uniquely identify security policy attributes. It shall also provide a means of listing all these attributes for a user, and all the users associated with an attribute. It shall be capable of defining and maintaining the security policy attributes for subjects including: defining and maintaining privileges for privileged subjects, discretionary and non-discretionary attributes, i.e., definition and maintenance of **roles**, and centralized distribution, review and revocation of policy attributes.

System administrators shall be provided with a protected mechanism for the purposes of granting and revoking user membership to specific roles. Administrative users shall also be provided with tools for the creation of roles and for the definition of role attributes.

4. The TCB shall support separate operator and administrator functions. The operator functions shall be restricted to those necessary for performing routine operations. The operator functions allow the enabling and disabling of peripheral devices, mounting of removable storage media, backing-up and recovering user objects; maintaining the TCB hardware and software elements (e.g., on site testing); and starting and shutting down the system.

5. The use of the protected mechanisms for system administration shall be limited to authorized administrative users. *The control of access-control attributes shall be limited to the object owner and to system administrators.*

3.7 Reference Mediation

Reference mediation, that is, the control by the TCB of subject accesses to objects, must be ensured so that the users can have faith in the TCB's access control decisions. Also, users must be ensured that all access to security services are mediated by the TCB.

For the CS3 level, RM-1 was assigned from the Federal Criteria. No refinements were made from CS2 or the Federal Criteria.

RM-1 Mediation of References to a Defined Subject/Object Subset

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.

2. Reference mediation shall include references to the defined subset of subjects, objects, and resources protected under the TCB security policy, and to their policy attributes, ***i.e., role identifiers***.

3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

3.8 Resource-Allocation Requirements

This component restricts the allocation of subjects and objects so that no one user through the exhaustion of resource can deny service to other users. It further enables the TCB to prioritize subject access to resources so that the highest priority subject is given preferential treatment in its access to objects.

For CS3l, AR-1 was assigned from the Federal Criteria. This component was refined from the Federal Criteria by limiting the control of the capability to place restrictions on the number of subjects and objects to system administrators.

LEVEL - AR-1 Resource Restrictions

The TCB shall provide the capability to place restrictions on the number of subjects and objects a user may have allocated at any given time. ***The control of this capability shall be limited to system administrators.*** The TCB shall control a defined set of system resources (e.g., memory, disk space) such that no one individual user can deny access to another user's subject and object space. All subjects, objects, and resources shall be defined with default space or time quota and number-of-resources attributes.

3.9 TCB Protection

TCB protection is a fundamental requirement for a secure product. All of the security components and mechanisms that have been described depend upon the integrity of the TCB and on the TCB being isolated and non-circumventable. The TCB must be resistant to outside penetration.

For the CS3 level, P-1 was assigned from the Federal Criteria. No refinements were made from CS2 or the Federal Criteria.

P-1 Basic TCB Isolation

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Noncircumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

3.10 Physical TCB Protection

Whenever the physical security of a product cannot be established, then all of the software controls that have been put into place are of no consequence. Therefore, physical TCB protection is just as important as software protection. Physical protection is based on a product's ability to prevent, deter, detect, and counter physical attacks against the product. Devices used to counter physical attacks must be shown to be tamper-resistant and non-circumventable.

For the CS3 level, PP-1 was assigned from the Federal Criteria. No further refinements were made from the Federal Criteria.

PP-1 Administrative and Environment Protection

1. Administrative procedures and environmental features necessary for establishing the physical security of a product's TCB shall be defined.

2. Product functions and devices necessary to establish physical control over the product's TCB shall be identified and provided.

3.11 TCB Self-Checking

Validating the correct operation of the TCB firmware and hardware is an important aspect of guaranteeing the integrity of the product. Hardware and software features that validate the correct operation of the product will be delivered with the product to ensure that the hardware and firmware are installed properly and are in working order.

For the CS3 level, SC-2 was assigned from the Federal Criteria. The refinements from CS2 and the Federal Criteria include providing for an encryption mechanism to preserve the integrity of object data and providing for a tool to check for storage medium and file system integrity, and for having system operators perform operator-controlled tests. An assignment was made to the configurable software features to monitor system services and the corruption of access control information.

SC-3 Software-Test Support

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB. These features shall include: power-on tests, loadable tests, and operator-controlled tests.

The power-on tests shall test all basic components of the TCB hardware and firmware elements including memory boards and memory interconnections; data paths; busses; control logic and processor registers; disk adapters; communication ports; system consoles, and the keyboard speaker. These tests shall cover all components that are necessary to run the loadable tests and the operator-controlled tests.

The loadable tests shall cover: processor components (e.g., arithmetic and logic unit, floating point unit, instruction decode buffers, interrupt controllers, register transfer bus, address translation buffer, cache, and processor-to-memory bus controller); backplane busses; memory controllers; writable control memory for operator-controlled and remote system-integrity testing.

Operator-controlled tests shall be able to initiate a series of one-time or repeated tests, to log the results of these tests and, if any fault is detected, to direct the integrity-test programs to identify and isolate the failure.*The execution of operator-controlled tests shall be limited to system* ***operators.***

Configurable software or firmware features shall be provided that can be used to validate the correct operation of the on-site software elements (i.e., code and data structures) of the TCB. These features may include, but are not limited to, checksums and consistency checks for TCB elements stored on storage media (e.g., disk-block consistency invariants).

a. At a minimum, these features shall also address:

(1) Monitoring of system services

(2) Corruption of access control information.

The TCB should provide an encryption mechanism that can be used to preserve the integrity of data in an object. (A)

The TCB shall provide tools for checking storage medium and file system integrity.

a. The TCB shall execute these tools periodically.

3.12 TCB Initialization and Recovery

The recovery and start-up of the TCB must be ensured so that the product always remains in a secure state, whether the recovery is performed manually or automatically.

For the CS3 level, TR-2 was assigned from the Federal Criteria. An assignment was made at this component level to specify that audit control data shall survive system restarts.

TR-3 Automated Recovery or Start-up

1. Procedures and/or mechanisms shall be provided to assure that, after a TCB failure or other discontinuity, recovery without protection compromise is obtained. ***At a minimum, audit control data (e.g., audit event masks) shall survive system restarts.***

2. Automated procedures, under the control of the TCB, shall be provided to assure that after a system failure, other discontinuity, or start-up, a secure state is obtained without undue loss of system or user objects. The security policy properties, or requirements, used to determine that a secure state is obtained shall be defined.

3.13 Privileged Operation

Privileges are associated with functional components so that at any given time only those operations that are associated with the privilege can be performed. The privileges that a product needs must be identified and must cover all the security aspects of the product, including the secure administration of the product, and should be defined so that there is not a single privileged mode for all of the TCB's operations.

For the CS3 level, PO-2 was assigned from the Federal Criteria. A refinement was made from CS2 and the Federal Criteria by specifying that privileges be associated with administrative roles and for controlling access to role registration files.

PO-2 Privilege Association with TCB Modules

1. TCB privileges needed by individual functions, or groups of functions, of a functional component shall be identified. Privileged TCB calls or access to privileged TCB objects, such as user and group ***and role*** registration files, password files, security and integrity-level definition file, role definition file, audit-log file shall also be identified. It shall be possible to associate TCB privileges with TCB operations performed by administrative users ***(i.e., administrative roles)***.

2.The modules of a TCB function shall be associated only with the privileges necessary to complete their task.

3. Support for product privilege implementation and association with TCB modules provided by lower-level mechanisms or procedures (e.g., operating system, processors, language) shall be provided.

3.14 Ease-of-TCB-Use

If security mechanisms are not easy to use and maintain, then administrative and non-system administrators may be tempted to disable the security mechanisms. Therefore, ease of use becomes an important element in the administration of a secure product and in the creation of privileged applications. It also minimizes errors on the part of both the administrative and non-system administrators, and can serve to minimize the consequences of these errors.

For the CS3 level, EU-3 was assigned from the Federal Criteria. No refinements were made from CS2 or the Federal Criteria.

EU-3 Common Configuration Coverage

> 1. The TCB shall provide well-defined actions to undertake administrative functions. Fail-safe default options shall be provided for security parameters of administrative functions.
>
> The TCB shall include fail-safe defaults for the policy attributes of subjects, objects (e.g., devices) and services used in common system configurations, as well as user-setable defaults for these subjects and objects.
>
> 2. The TCB shall provide well-defined application programming interfaces and programming functions (e.g., libraries) for all its policies to support the development of applications that can define and enforce security policies on application-controlled subjects and objects. The TCB shall enable user-controlled reduction of permissions available to applications.

CS3 Assurance

4. Introduction

This chapter provides the CS3 development and evaluation assurance requirements package using the development and evaluation assurance components defined in Volume I and the package contained in Volume I, Appendix G of the Federal Criteria. The structure of each assurance package follows that of the assurance components (i.e., each package consists of development process, operational support, development environment, development evidence, and evaluation process components).

Assurance Package T3+

The enhanced assurance level is intended to include the best of the commercial computer products designed to satisfy functional requirements. As such this package includes several extensions to the assurance components of the previous two packages.

The intent of product development assurance for this package is both to establish that the external behavior of the product conforms to its user level and administrative documentation and to provide visibility into the internal structure of the product TCB. For this reason, requirements for Descriptive Interface Specifications (DIS) and modular decomposition have been added. The TCB element identification and functional testing, have also been extended and penetration testing requirements added to support the added assurances of external behavior.

The intent of the operational support assurance for this package is to establish a level of user and administrative guidance and product information that enables the correct product installation and use of product security features. The developer is required to establish and document a policy for responding to customer inquiries and flaw remediation. Similarly, the development environment assurances are intended to provide the a level of control over the product configuration and production, including well-defined coding standards and strict configuration management processes. This level of development environment assurance is similar to that used in the most advanced commercial development organizations.

The development evidence required for this package is commensurate with the assurances required. The intent of this package is to require the type of assurance evidence that is generated during commercial development oriented towards of high-quality products.

The intent of evaluation support assurance is to establish that the product, and the context in which it is developed and supported, is commensurate with the development assurance requirements. At the T3+ level, testing analysis and the requirement for independent testing determines whether the product meets the functional protection requirements. Operational support evaluation assurance determines whether the product documentation correctly describes the security relevant operations. Development environment assurance determines whether the product meets the requirements as defined in the protection profile's development assurance subsections. Design assurance determines whether the product meets the design requirements as defined in the Development Process Assurance section of this Protection Profile.

Also for CS3, flaw remediation was included in this package. Flaw remediation is important for commercial environments since it ensures that flaws (i.e, deficiencies in a product that enables a user external to the TCB to violate the functional requirements of a protection profile) that are discovered by the product consumers will be tracked, corrected, and disseminated to the affected customers.

The following table summarizes the assurance components that comprise T3+. Note that this package is indicated as being T3+ since an additional component was included for flaw remediation. Also note that the requirement for role based administrative guidance was included from level AG-3 and is indicated in the table below as "AG-2+" and in the component text by the insertion of "[AG-3]"at the beginning of the paragraph.

.

CS3 Assurance Package

Assurance Component Summary	T3+
Development Process	
TCB Property Definition	PD-2
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-1

CS3 Assurance Package

Assurance Component Summary	T3+
TCB Modular Decomposition	----
TCB Structuring Support	SP-1
TCB Design Disciplines	----
TCB Implementation Support	----
TCB Testing & Analysis	
Functional Testing	FT-1
Penetration Analysis	PA-1
Covert Channel Analysis	----
Operational Support	
User’s Security Guidance	UG-1
Administrative Guidance	AG-2+
Flaw Remediation	FR-2
Trusted Generation	TG-2
Development Environment	
Life Cycle Definition	LC-1
Configuration Management	CM-1
Trusted Distribution	---
Development Evidence	
TCB Protection Properties	EPP-1
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	EPA-1
Covert Channel Analysis	----
Product Support	EPS-2
Evaluation Process	
Testing	
Test Analysis	TA-2
Independent Testing	IT-1
Review	
Development Environment	DER-1
Operational Support	OSR-1
Analysis	
Protection Properties	---
Design	DA-1
Implementation	----

4.1 TCB Property Definition

The definition of TCB properties assures the consistency of the TCB's behavior. It determines a baseline set of properties that can be used by system developers and evaluators to assure that the TCB satisfies the defined functional requirements.

For CS3, PD-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

PD-2 Informal Property Definition

> The developer shall provide informal models for the functional components and sub-components of the profile. At a minimum, an informal model of the access control components shall be provided. Each informal model shall include (abstract) data structures and operations defining each functional component or sub-component, and a description of the model properties. The developer shall interpret (e.g., trace) the informal models within the product TCB. For each model entity, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that entity; (2) define the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the model properties. The developer's interpretation of each informal model, which defines the TCB properties, shall identify all TCB elements that do not correspond to any model entity and shall explain why these elements do not render the TCB properties invalid.
>
> For the components that are not informally modeled, the developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement. The developer's interpretation of each functional requirement, which describes the TCB properties, shall identify all TCB elements that do not correspond to any functional requirement and shall explain why these elements do not render the TCB properties invalid.

4.2 TCB Element Identification

The identification of TCB elements (hardware, firmware, software, code, and data structures) provides the set of elements that determine the protection characteristics of a product. All assurance methods rely on the correct identification of TCB elements either directly or indirectly.

For CS3, ID-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

ID-2: TCB Element Justification

> The developer shall identify the TCB elements (i.e., software, hardware/firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).
>
> The developer shall justify the protection relevance of the identified elements (i.e., only elements that can affect the correct operation of the protection functions shall be included in the TCB). If protection-irrelevant elements are included in the TCB, the developer shall provide a rationale for such inclusion.

4.3 TCB Interface Definition

The TCB interface establishes the boundary between the TCB and its external users and application programs. It consists of several components, such as command interfaces (i.e., user oriented devices such as the keyboard and mouse), application program interfaces (system calls), and machine/processor interfaces (processor instructions).

For CS3, IF-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

IF-1: Interface Description

> The developer shall describe all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB. The description shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.
>
> The developer shall identify all call conventions (e.g., parameter order, call sequence requirements) and exceptions signaled at the TCB interface.

TCB Structuring Support

Structuring the TCB into modules is necessary. However, the modular decomposition does not necessarily reflect the run-time enforcement of the TCB structuring since the separation of modules may not necessarily be supported by run-time mechanisms. The run-time enforcement of internal TCB structuring adds a measure of assurance that the TCB elements that are critical to the enforcement of the protection functions are separate from the non-critical elements. Also, the use of run-time enforcement of TCB structuring helps separate protection-critical TCB elements from each other, thereby helping to enforce the separation of protection concerns and minimizing the common mechanisms shared between protection critical elements.

For CS3, SP-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

SP-1: Process Isolation

> The TCB shall maintain process isolation.

4.4 Developer Functional Testing

Functional testing establishes that the TCB interface exhibits the properties necessary to satisfy the requirements of the protection profile. It provides assurance that the TCB satisfies at least its functional protection requirements.

For CS3, FT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

FT-1: Conformance Testing

> The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description.
>
> The developer shall correct all flaws discovered by testing and shall retest the TCB until the protection functions are shown to work as claimed.

4.5 Penetration Analysis

Penetration analysis is an important assurance component since the effectiveness of all security policies rely on the penetration resistance of the TCB. TCB penetration analysis consists of the identification and confirmation of flaws in the design and implementation of protection functions that can be exploited by unprivileged users or untrusted application programs.

For CS3, PA-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

PA-1 Basic Penetration Testing

> The developer shall define the TCB configuration, interface, and protection functions that are subject to penetration testing. For each test, the developer shall identify the goal of the test and the criteria for successful penetration. The developer shall identify all product documentation (e.g., system reference manuals) used to define penetration-test conditions, and shall document all test conditions, data (e.g., test set-up, function call parameters, and test outcomes), and coverage.
>
> The penetration testing shall include, at a minimum, known classes of penetration flaws found in other TCBs (e.g., generic penetration flaws). For each uncovered flaw, the developer shall define and document scenarios of flaw exploitation, and shall identify all penetration outcomes resulting from that scenario.

4.6 User’s Guidance

User’s guidance is an operational support assurance component that ensures that usage constraints assumed by the protection profile are understood by the users of the product. It is the primary means available for providing product users with the necessary background and specific information on how to correctly use the product’s protection functionality.

For CS3, UG-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

UG-1: Users' Guide

> The developer shall provide a Users' Guide which describes all protection services provided and enforced by the TCB. The User's Guide shall describe the interaction between these services and provide examples of their use. The User's Guide may be in the form of a summary, chapter or manual. The User’s Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

4.7 Administrative Guidance

Administrative guidance is an operation support assurance component that ensures that the environmental constraints assumed by the protection profile are understood by administrative users and operators of the IT product. It is the primary means available to the developer for providing to administrators and operators detailed, accurate information on how to configure and install the product, operate the IT product is a secure manner, make effective use of the product's privileges and protection mechanisms to control access to administrative functions and data bases, and to avoid pitfalls and improper use of the administrative functions that would compromise the TCB and user security.

For CS3, AG-2+ was assigned from the Federal Criteria. This level is indicated as being "AG-2+" because requirements were included from AG-3 for role based administrative guidance. This is indicated in the text by an *"[AG-3]"* in front of the paragraph and through the use of ***bold italics***.

AG-2+: Detailed Administrative Guidance

> ***[AG-3]:*** The developer shall provide a Trusted Facility Manual intended for the product administrators and operators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB. The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy. The Trusted Facility Manual shall explain the unique security-relevant privileges and functions of administrators and operators. ***The Trusted Facility Manual shall also explain the distinct security-relevant privileges and functions of the TCB and how they can be selectively granted to provide fine-grained, multi-role system and application administration policies.*** The Trusted Facility Manual shall describe the administrative interaction between security services.
>
> The Trusted Facility Manual shall identify all hardware, firmware, software, and data structures comprising the TCB. The detailed audit record structure for each type of audit event shall be described. If covert channel handling is required, the Trusted Facility Manual shall explain how configure the product to mitigate, eliminate, or audit covert channel exploitation.The Trusted Facility Manual shall describe the cautions about and procedures for using the TCB as a base for site-specific secure applications. The Trusted Facility Manual shall describe procedures for securely regenerating the TCB after any part is changed (e.g., due to adding devices or installing flaw corrections to the TCB software).
>
> The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.

4.8 Flaw Remediation Procedures

Flaw remediation is an operational support assurance component that ensures that flaws (i.e, deficiencies in the product that enable a user external to the TCB to violate the functional requirements of a protection profile) that are discovered by the product consumers will be tracked and corrected while the product is supported by the developer.

For CS3, FR-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

FR-2: Flaw Reporting Procedures

Flaw Tracking Procedures: The developer shall establish a procedure to track all reported protection flaws with each release of the product. The tracking system shall include a description of the nature and effect of each flaw and the status of finding a correction to the flaw.

Flaw Repair Procedures: The developer shall establish a procedure to identify corrective actions for protection flaws. This procedure shall include a policy to separate protection-relevant from non-protection relevant corrections, changes, or upgrades to the product.

Consumer Interaction Procedures: The developer shall establish a procedure for accepting consumer reports of protection problems and requests for corrections to those problems. The developer shall designate one or more specific points of contact for consumer reports and inquiries about protection issues involving the product. This procedure and the designated points of contact shall be provided in the consumer documentation (e.g., the TFM or the SFUG).

4.9 Trusted Generation

Trusted generation is an operational support assurance component that ensures that the copy of the product's TCB that is configured and activated by the consumer exhibits the same protection properties as the master copy of the product's TCB that was evaluated for compliance with the protection profile. The trusted generation procedures must provide some confidence that the consumer will be aware of what product configuration parameters can affect the protection properties of the TCB. The procedures must encourage the consumer to choose parameter settings that are within the bounds assumed during the product evaluation.

For CS3, TG-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

TG-2: Trusted Generation With Fail-Safe Defaults

> The developer shall establish and document the procedures that a customer must perform to generate an operational TCB from the delivered copy of the master TCB. The customer documentation shall identify any system parameters, which are initialized or set during system generation, that affect the TCB's conformance to the protection profile and state the acceptable ranges of values for those parameters. The product shall be delivered with each of these parameters set to its fail-safe defaults.

4.10 Life Cycle Definition

Life cycle definition is an assurance component for establishing that the business practices used by a developer to produce the product's TCB include the considerations and activities identified by the development process and operational support requirements of the protection profile. Consumer confidence in the correspondence between the protection profile requirements and the product's TCB is greater when security analysis and the production of evidence are done on a regular basis as a integral part of the development process and operational support activities.

For CS3, LC-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

LC-1: Developer-Defined Life Cycle Process

> The developer shall describe the process used to develop and maintain the product. The process shall incorporate a security policy that states the technical, physical, procedural, personnel, and other measures used by the developer to protect the product and its documentation. The developer shall trace each development process and support process requirement of the protection profile to the part, or parts, of the developer's process where the requirement is satisfied. The developer shall identify the programming languages used to develop the TCB software.

4.11 Configuration Management

Configuration management is an assurance component that ensures that the product's TCB configuration remains consistent and complete, and that changes to the TCB do not adversely affect the protection properties of the TCB. Configuration management must ensure that additions, deletions, or changes to the TCB do not compromise the correspondence between the TCB's implementation and the requirements of the protection profile. This is accomplished by requiring the developer to have procedures or tools that ensure that the TCB and its documents are updated properly with the TCB changes.

For CS3, CM-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

CM-1: Procedural Control and Generation

> The developer shall establish configuration control and generation procedures for developing and maintaining the TCB. The procedures shall be employed to ensure that changes to the TCB are consistent with the product's protection properties and security policy. The developer shall employ these procedures to track changes to development evidence, implementation data (e.g., source code and hardware diagrams), executable versions of the TCB, test documentation and procedures, identified flaws, and consumer documentation.
>
> The configuration control procedures shall permit the regeneration of any supported version of the TCB.

4.12 Evidence of TCB Protection Properties

The documentation of the TCB protection properties includes the definition of the functional component requirements, their modeling (if any), and their interpretation within a product's TCB. For each requirement of a protection profile, a description, definition (an informal, descriptive specification), or a formal specification of the TCB components and their operation corresponding to the requirement must be provided.

For CS3, EPP-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPP-2 Evidence of Informal Model Interpretation in the TCB

> The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. The developer shall also provide an informal access control model and its interpretation within the TCB. The TCB properties, which are defined by this correspondence, shall be explained in this documentation.

4.13 Evidence of Product Development

Product development evidence consists of the TCB design evidence including the documentation of the TCB interface, TCB elements, TCB structure, TCB structuring support, and TCB design disciplines. The TCB implementation evidence includes TCB source code, and the processor hardware and firmware specifications.

For CS3, EPD-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPD-1: Description Of The TCB External Interface

> The developer shall provide an accurate description of the functions, effects, exceptions and error messages visible at the TCB interface.
>
> The developer shall provide a list of the TCB elements (hardware, software, and firmware).

4.14 Evidence of Functional Testing

Functional testing evidence includes the testing itself, the test plans, and test documentation results. Test plans consist of: the description definition or specification of the test conditions; the test data, which consists of the test environment set-up; the test parameters and expected outcomes; and a description of the test coverage.

For CS3, EFT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EFT-1: Evidence of Conformance Testing

> The developer shall provide evidence of the functional testing that includes the test plan, the test procedures and the results of the functional testing.

4.15 Evidence of Penetration Analysis

The penetration analysis evidence includes, in addition to penetration test plans and results configured in the same manner as the functional testing evidence, the documentation of the penetration-resistance testing methods and tools, conditions that were verified, the outcomes of the verification and, when appropriate, the scenario of the discovered penetration flaws. The cause of every discovered penetration flaw, or class of penetration flaws, must also be documented.

For CS3, EPA-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPA-1: Evidence of Penetration Testing

> The developer shall provide evidence of penetration testing. The evidence shall identify all product documentation on which the search for flaws was based. The penetration evidence shall describe the scenarios for exploiting each potential flaw in the system and the penetration test conditions, data (e.g., test set-up, function call parameters, and test outcomes), coverage, and conclusions derived from each scenario.

4.16 Evidence of Product Support

Product support evidence consists of the development environment and operational support documentation and tools. The development environment evidence includes the documentation of the product life-cycle process, configuration management procedures enforced, and the trusted distribution mechanisms and procedures used. It also includes: the identification of the tools used in the product development, configuration management, and trusted distribution; and the characteristics that make those tools suitable for the development of product protection.

For CS3, EPS-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

EPS-1: Evidence of Basic Product Support

> The developer shall provide evidence that describes the policies, procedures, and plans established by the developer to satisfy the Operational Support and Development Environment requirements of the protection profile.

4.17 Test Analysis

Test analysis determines whether the product meets the functional protection requirements defined in the protection profile. Functional testing is based on operational product, the TCB’s functional properties, the product’s operational support guidance, and other producer's documentation as defined by the development evidence requirements. Functional test analysis is based on the achieved test results as compared to the expected results derived from the development evidence.

For CS3, TA-2 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

TA-2: Enhanced Test Analysis

> The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and penetration analysis, and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results, and general correctness (e.g., defect trend from regression testing). This analysis shall examine the testability of requirements, the adequacy of the tests to measure the required properties, the deviation of the actual results obtained from the expected results, and a general interpretation of what the testing results mean. The evaluator shall determine whether the product's protection properties, as described in the product documentation, and all relevant known penetration flaws have been tested. The evaluator shall assess testing results to determine whether the product’s TCB works as claimed, and whether there are any remaining obvious ways (i.e., ways that are known, or that are readily apparent or easily discovered in product documentation) for an unauthorized user to bypass the policy implemented by the TCB or otherwise defeat the product’s TCB.

4.18 Independent Testing

Independent testing determines whether the product’s TCB meets the functional protection requirements as defined in the functionality chapter of this Protection Profile. Testing is based on operational product, the TCB’s functional properties, the product’s operational support guidance, and other producer's documentation as defined by the Development Evidence requirements.

For CS3, IT-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

IT-1: Elementary Independent Testing

> A tester, independent of the producer or evaluator, shall perform functional and elementary penetration testing. This testing shall be based on the product's user and administrative documentation, and on relevant known penetration flaws. Satisfactory completion consists of demonstrating that all user-visible security enforcing functions and security-relevant functions work as described in the product's user and administrative documentation and that no discrepancies exist between the documentation and the product. Test results of the producer shall be confirmed by the results of independent testing. The evaluator may selectively reconfirm any test result.
>
> If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results. The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results. The evaluator shall confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.

4.19 Development Environment Review

Development environment review determines whether the product meets the requirements as defined in the protection profile’s Development Assurance subsections for Development Environment including Life-Cycle Definition and Configuration Management.

For CS3, DER-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

DER-1: Elementary Development Environment Review

> The evaluator shall review the producer's development and maintenance process description documentation to determine the degree of discipline enforced upon and within the process, and to determine the protection characteristics associated with the product's development and maintenance. The results of this review shall establish, for the evaluator, the producer’s development environment, its policies, and the degree of enforcement maintained during development execution.

4.20 Operational Support Review

Operation support review establishes the level of review required to determine whether the product meets the requirements as defined in the protection profile's Development Assurance subsections for Operational Support including, at the CS3 level, the User and Administrative Guidance documents.

For CS3, OSR-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

OSR-1 Elementary Operational Support Review

> The evaluator shall review all documentation focused on the activities of product use (e.g., Users Manuals) and product administration including installation, operation, maintenance, and trusted recovery (e.g., Trusted Facility Management Manuals). This review shall assess the clarity of presentation, difficulty in locating topics of interest, ease of understanding, and completeness of coverage. The need for separate manuals dedicated to protection-relevant aspects of the product should be assessed for effectiveness.
>
> This component should also address flaw remediation and trusted generation. [[TBD.]]

4.21 Design Analysis

Design analysis determines whether the product meets the design requirements as defined in the Development Process Assurance section of the protection profile, including the TCB Property Definition and TCB Design requirements. The analysis is based on the producer's documentation, as defined by the Development Evidence requirements.

For CS3, DA-1 was assigned from the Federal Criteria. No refinements were made from the Federal Criteria.

DA-1: Elementary Design Analysis

> The evaluator shall determine whether the producer has performed the activities defined in the development process assurance requirements of the protection profile for TCB property definition and TCB design. The evaluator shall determine whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's activities for completeness and consistency of design with respect to requirements.

GLOSSARY

Access - Ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or object in an Information Technology (IT) Product. Frequently used as a verb, contrary to the rules of grammar.

Note: An individual does not have "access" if the proper authority or a physical, technical, or procedural measure prevents them from obtaining knowledge or having an opportunity to alter information, material, resources, or components.

Access Control - Process of limiting access to the resources of an IT product only to authorized users, programs, processes, systems, or other IT products.

Access Control List -A list of subjects that are authorized to have access to some object(s). Usually, this list contains entries consisting of identifiers of users and groups of users and access rights.

Access Control Mechanism - Security safeguards designed to detect and prevent unauthorized access, and to permit authorized access in an IT product.

Access Mediation - Process of monitoring and controlling access to the resources of an IT product, including but not limited to the monitoring and updating of policy attributes during accesses as well as the protection of unauthorized or inappropriate accesses (see Access Control).

Accountability - Means of linking individuals to their interactions with an IT product, thereby supporting identification of and recovery from unexpected or unavoidable failures of the control objectives.

Accreditation - Formal declaration by a designated approving authority that an Automated Information System (AIS) is approved to operate in a particular security configuration using a prescribed set of safeguards.

Application Program Interface - System access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Assignment - Requirement in a protection profile taken directly as stated, without change, from the list of components or derived by placing a bound on a threshold definition.

Note: The assignment of environment-specific requirements to generic component requirements is performed when a component requirement corresponds to an environment-specific requirement.

Assurance - (See Profile Assurance and IT Product Assurance).

Audit - Independent review and examination of records and activities to determine compliance with established usage policies and to detect possible inadequacies in product technical security policies of their enforcement.

Audit Trail - Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. [NSTISSI 4009]

Note: Audit trail may apply to information in an IT product or an AIS or to the transfer of COMSEC material.

Authenticate - Verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT product.

Authentication - Means of verifying an entity's (e.g., individual user, machine, software component) eligibility to receive specific categories of information.

Authorization - Access rights granted to a user, program, or process. [NSTISSI 4009]

Authorized - Entitled to a specific mode of access.

Automated Information System (AIS) - Any equipment or interconnected systems or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware. [NSTISSI 4009]

Note: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Availability - Ability to access a specific resource within a specific time frame as defined within the IT product specification.

Bandwidth - Rate at which information is transmitted through a channel. (See channel capacity)

Note: Bandwidth is originally a term used in analog communication, measured in Hertz, and related to information rate by the "sampling theorem" (generally attributed to H. Nyquist although the theorem was in fact known before Nyquist used it in communication theory). Nyquist's sampling theorem says that the information rate in bits (samples) per second is at most twice the bandwidth in Hertz of an analog signal created from a square wave. In a covert-channel context "bandwidth" is given in bits/second rather than Hertz and is commonly used, in an abuse of terminology, as a synonym for information rate.

Bell-La Padula Security Model - Any formal state-transition model of a technical security policy for an AIS that presents (a) Access Constraints (including initial-state constraints and variants or the simple security and star properties), (b) allowed state transitions (called "rules of operation"), and (c) a proof that the allowed state transitions guarantee satisfaction of the constraints.

Category - Restrictive label that has been applied to both classified and unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data. [NSTISSI 4009]

Note: Examples include sensitive compartmented information and proprietary information. Individuals are granted access to special category information only after being granted formal access authorization.

Certification - Comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NSTISSI 4009]

Channel Capacity - Maximum possible error-free rate, measured in bits per second, at which information can be sent along a communications path.

Clear-text - Intelligible data, the semantic content of which is available. [ISO]

Confidentiality - Assurance that information is not disclosed to inappropriate entities or processes.

Configuration - Selection of one of the sets of possible combinations of features of a system. [ITSEC]

Consumers - Individuals or groups responsible for specifying requirements for IT product security (e.g., policy makers and regulatory officials, system architects, integrators, acquisition managers, product purchasers, and end users.

Control Objective - Required result of protecting information within an IT product and its immediate environment.

Countermeasure - Action, device, procedure, technique, or other measure that reduces the vulnerability of an AIS. [NSTISSI 4009]

Covert Channel - Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an AIS security policy. (See overt channel and exploitable channel.) [NSTISSI 4009]

Covert Storage Channel - Covert channel that involves the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. [NSTISSI 4009]

Note: Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel - Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process. [NSTISSI 4009]

Decomposition - Requirement in a protection profile that spans several components.

> Note: The decomposition of a specific requirement becomes necessary when that requirement must be assigned to multiple components of the generic product requirements during the interpretation process.

Definition - an informal statement expressing the essential characteristics of one or more facts.

Demonstration - an act or process of producing conclusive evidence for one or more facts. (A demonstration is more rigorous than an explanation and less rigorous than a proof).

Dependency - Condition in which the correctness of one or more functions (or assurances) is contingent (depends for its correctness) on the correctness of another function(s) (or assurances). Notion also used in describing the relationships among TCB subsets [NCSC-TG-021]. A TCB subset ***A*** depends for its correctness on TCB subset ***B*** if and only if the (engineering) arguments of the correct implementation of ***A*** with respect to its specification assume, wholly or in part, that the specification of ***B*** has been implemented correctly.

Description - an enumeration of facts and their characteristics.

Designated Approving Authority (DAA) - Official with the authority to formally assume responsibility for operating an IT product, an AIS, or network at an acceptable level of risk.

Development Assurance - Sources of IT product assurance ranging from how a product was designed and implemented to how it is tested, operated and maintained.

Development Assurance Component - Fundamental building block, specifying how an IT product is developed, from which development assurance requirements are assembled.

Development Assurance Package - Grouping of development assurance components assembled to ease specification and common understanding of how an IT product is developed.

Development Assurance Requirements - Requirements in a protection profile which address how each conforming IT product is developed including the production of appropriate supporting developmental process evidence and how that product will be maintained.

Discretionary Access Control - Methods of restricting access to objects or other resources based primarily on the instructions of arbitrary unprivileged users.

Domain - Unique context (e.g., access control parameters) in which a program is operating.

> Note: A subject's domain determines which access-control attributes an object must have for a subject operating in that domain to have a designated form of access.

Encapsulated Object -A data structure whose existence is known, but whose internal organization is not accessible, except by invoking the encapsulated subsystem that manages it.

Encapsulated Subsystem -A collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the encapsulated subsystem that the procedures may be called only at designated domain entry points. Encapsulated subsystem, protected subsystem, and protected mechanisms of the TCB are terms that may be used interchangeably.

Environment - All entities (users, procedures, conditions, objects, AISs, other IT products) that interact with (affect the development, operation and maintenance of) that IT product.

Evaluation - Technical assessment of a component's, product's, subsystem's, or system's security properties that establishes whether or not the component, product, subsystem, or system meets a specific set of requirements.

> Note: Evaluation is a term that causes much confusion in the security community, because it is used in many different ways. It is sometimes used in the general English sense (judgement or determination of worth or quality). Based on common usage of the term in the security community, one can distinguish between two types of evaluation: (1) evaluations that exclude the environment, and (2) evaluations that include the environment. This second type of evaluation, an assessment of a system's security properties with respect to a specific operational mission, is termed *certification* within this document. Evaluations that exclude the environment, the type of evaluations considered herein, are assessments of the security properties against a defined criteria.

Evaluation Assurance - Source of IT product assurance based on the kind and intensity of the evaluation analysis performed on the product.

Evaluation Assurance Component - Fundamental building block, specifying the type and the rigor of required evaluation activities, from which evaluation assurance requirements are assembled.

Evaluation Assurance Package - Grouping of evaluation assurance components assembled to ease specification and common understanding of the type and the rigor of required evaluation activities.

Evaluation Assurance Requirements - Requirements in a protection profile which address both the type and the rigor of activities that must occur during product evaluation.

Evaluators - Individuals or groups responsible for the independent assessment of IT product security (e.g., product evaluators, system security officers, system certifiers, and system accreditors).

Explanation - a description and its justification; an enumeration of facts, their characteristics, and their cause or reason. (An explanation is less rigorous than both a demonstration and a proof.)

Exploitable Channel - Covert channel that is usable or detectable by subjects external to the AIS's trusted computing base and can be used to violate the AIS's technical security policy. (See covert channel.)

External Security Controls - Measures which include physical, personnel, procedural, and administrative security requirements and a separate certification and accreditation process that govern physical access to an IT product.

Note: These measures constitute assumptions and boundary conditions that are part of the environment described in a protection profile.

Flaw - Error of commission, omission, or oversight in an IT product that may allow protection mechanisms to be bypassed.

Formal Security Policy Model - Mathematically precise statement consisting of (a) a formal technical security policy (given by constraints on a Product's external interface and/or constraints on the handling of controlled entities internal to the Product), (b) rules of operation that show how the definition of security is to be enforced, and (c) a formal proof showing that the rules of operation guarantee satisfaction of the definition of security. [NCSC-TG-010]

Formal Specification - Statement about a product made using the restricted syntax and grammar of a formal reasoning system and a set of terms that have been precisely and uniquely defined of specified.

Note: The formal statement should be augmented by an informal explanation of the conventions used and the ideas being expressed. A well-formed syntax and semantics with complete specification of all constructs used must be referenced.

Functional Component - Fundamental building block, specifying what an IT product must be capable of doing, from which functional protection requirements are assembled.

Functional Package - Grouping of functional components assembled to ease specification and common understanding of what an IT product is capable of doing.

Functional Protection Requirements - Requirements in a protection profile which address what conforming IT products must be capable of doing.

Functionality - Set of functional protection requirements to be implemented in IT products.

Generic Threat - Class of threats with common characteristics pertaining to vulnerabilities, agents, event sequences, and resulting misfortunes.

Granularity - Relative fineness or coarseness to which an access control mechanism or other IT product aspect can be adjusted.

Note: Protection at the file level is considered course granularity, whereas protection at the field level is considered to be finer granularity.

Granularity of a Requirement - Determination of whether a requirement applies to all the attributes of users, subjects or objects, and all TCB functional components.

Group - Named collection of user identifiers.

Identification - Process that enables recognition of an entity by an IT product.

Informal Specification - Statement about (the properties of) a product made using the grammar, syntax, and common definitions of a natural language (e.g., English).

Note: While no notational restrictions apply, the informal specification is also required to provide defined meanings for terms which are used in a context other than that accepted by normal usage.

Information Protection Policy - Set of laws, rules, and practices that regulate how an IT product will, within specified limits, counter threats expected in the product's assumed operational environment.

Internal Security Controls - Mechanisms implemented in the hardware, firmware, and software of an IT product which provide protection for the IT product.

Integrity - Correctness and appropriateness of the content and/or source of a piece of information.

Least Privilege - Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. [NSTISSI 4009]

Note: Application of this principle limits the damage that can result from accident, error, or unauthorized use of an AIS.

Mandatory Access Control - Means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. (See non-discretionary access control.)

Mechanism - Operating system entry point or separate operating system support program that performs a specific action or related group of actions.

Need-to-know - Access to, or knowledge or possession of, specific information required to carry out official duties. [NSTISSI 4009]

Non-Discretionary Access Control - Means of restricting access to objects based largely on administrative actions.

Normal Operation - Process of using a system. [ITSEC]

Object - Controlled entity that precisely gives or receives information in response to access attempts by another (active) entity.

Note: Access to an object implies access to the information contained in that object. Examples of objects include: subjects, records, blocks, pages, segments, files, directories, directory trees and programs, as well as bits, bytes, words, fields, processors, I/O devices, video displays, keyboards, clocks, printers, and network nodes.

Object Encapsulation - viz., encapsulated object.

Organizational Security Policy - Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Overt Channel - Communications path within a computer system or network that is designed for the authorized transfer of data. (See covert channel) [NSTISSI 4009]

Owner - User granted privileges with respect to security attributes and privileges affecting specific subjects and objects.

Password - Protected/private character string used to authenticate an identity or to authorize access to data. [NSTISSI 4009]

Penetration Testing - Security testing in which evaluators attempt to circumvent the security features of an AIS based on their understanding of the system design and implementation. [NSTISSI 4009]

Primitive - Orderly relation between TCB subsets based on dependency. [NCSC-TG-021]

Note: A TCB subset ***B*** is more primitive than a second TCB subset ***A*** (and ***A*** is less primitive than ***B***) if ***A*** directly depends on ***B*** or a chain of TCB subsets from ***A*** to ***B*** exists such that each element of the chain directly depends on its successor in the chain.

Privilege - Special authorization that is granted to particular users to perform security relevant operations.

Process - A program in execution on a processor which represents a scheduling and accounting (and sometimes a concurrency and recovery) entity in a computer system.

Producers - Providers of IT product security (e.g., product vendors, product developers, security analysts, and value-added resellers).

Product - Package of IT software and/or hardware designed to perform a specific function either stand alone or once incorporated into an IT system.

Product Rationale - Overall justification; including anticipated threats, objectives for product functionality and assurance, technical security policy, and assumptions about the environments and uses of conforming products; for the protection profile and its resulting IT product.

Profile - Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IT product or AIS. (See Protection Profile.)

Profile Assurance - Measure of confidence in the technical soundness of a protection profile.

Proprietary Information - Information that is owned by a private enterprise and whose use and/or distribution is restricted by that enterprise.

Note: Proprietary information may be related to the company's products, business, or activities, including but not limited to: financial information, data or statements; trade secrets; product research and development information; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and trade secrets or other company confidential information.

Protected Mechanism - See encapsulated subsystem.

Protection Philosophy - Informal description of the overall design of an IT product that shows how each of the supported control objectives is dealt with.

Protection Profile - Statement of security criteria; shared by IT product producers, consumers, and evaluators; built from functional, development assurance, and evaluation assurance requirements; to meet identified security needs through the development of conforming IT products.

Protection Profile Family - Two or more protection profiles with similar functional requirements and rationale sections but with different assurance requirements.

Proof - the process of establishing the validity of one or more statements; the process of establishing a the truth of a fact. (A proof is more rigorous than both a demonstration and an explanation.)

Prove a Correspondence - Provide a formal correspondence, using a formal reasoning system (e.g., typed lambda calculus) between the levels of abstraction.

Note: This involves proving that required properties continue to hold under the interpretation given in the formal correspondence.

Reference Monitor - Access mediation concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Reference Validation Mechanism - Portion of a trusted computing base, the normal function of which is to mediate access between subjects and objects, and the correct operation of which is essential to the protection of data in the system.

Note: This is the implementation of reference monitor.

Refinements - Requirement in a protection profile taken to a lower level of abstraction than the component on which it is based.

Note: The refinement of a component requirement is necessary when multiple environment-specific requirements must be assigned to a single component requirement.

Requirements - Phase of the Development Process wherein the top level definition of the functionality of the system is produced.

Residual Risk - Portion of risk that remains after security measures have been applied. [NSTISSI 4009]

Resource - Anything used or consumed while performing a function.

Note: The categories of resources include: time, information, objects (information containers), or processors (the ability to use information) Specific examples include: CPU time; terminal connect time; amount of directly-addressable memory; disk space; and number of I/O requests per minute.

Risk - The expected loss due to, or impact of, anticipated threats in light of system vulnerabilities and strength or determination of relevant threat agents.

Role - A distinct set of operations (actions) performed on encapsulated data objects.

Scope of a Requirement - Determination of whether a requirement applies to: all users, subjects and objects of the TCB; all the TCB commands and application programming interfaces, to all TCB elements; all configurations, or only a defined subset of configurations.

Security - The combination of confidentiality, integrity and availability. [ITSEC]

Security kernel - An encapsulation of key security-relevant portions of an operating system that prevent unauthorized subject access to objects.

Security Audit Trail - Set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. [TCSEC]

Security Relevant Event - Any event that attempts to change the security state of the system (e.g., change access controls, change the security level of a user, change a user password). Also, any event that attempts to violate the security policy of the system (e.g., too many logon attempts). [TCSEC]

Security Target - Product-specific description, elaborating the more general requirements in a protection profile and including all evidence generated by the producers, of how a specific IT product meets the security requirements of a given protection profile.

Trace a Correspondence - Explain a correspondence, using natural language prose, between levels of abstraction.

Transaction - Set of subject actions and their associated data storage accesses.

Trap Door - Hidden software or hardware mechanism that can be triggered to permit protection mechanisms in an automated information system to be circumvented. [NSTISSI 4009]

Note: A trap door is usually activated in some innocent-appearing manner (e.g., a special random key sequence at a terminal). Software developers often write trap doors in their code that enable them to reenter the system to perform certain functions.

Trojan Horse - Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allow unauthorized collection, falsification or destruction of data. [NSTISSI 4009]

Trusted Computing Base (TCB) - Totality of protection mechanisms within an IT product, including hardware, firmware, software and data, the combination of which is responsible for enforcing a technical security policy.

Note: The ability of an organization to achieve an organizational security policy depends jointly on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and on adherence to associated usage security policies by authorized users.

Trusted Path - Mechanism by which a person using a terminal can communicate directly with the TCB. [NSTISSI 4009]

Note: Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.

Usage Security Policy - Assumptions regarding the expected environment and intended method of IT product use.

User - Person or process accessing an IT product by direct connections (e.g., via terminals) or indirect connections; an individual who is accountable for some identifiable set of activities in a computer system.

Note: *Indirect connection* relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual.

User Identifier (User ID)- Unique symbol or character string that is used by an IT product to uniquely identify a specific user.

Virus - Self replicating, malicious program segment that attaches itself to an application or other executable system component and leaves no external signs of its presence. [NSTISSI 4009]

Vulnerability - Weakness in an information system or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to produce an information-related misfortune.

CSR References

1. U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, December 1985.

2. Information Technology Security Evaluation Criteria (ITSEC) - Provisional Harmonized Criteria, Version 1.2, June 1991.

3. Bellcore Standard Operating Environment Security Requirements, TA-STS-001080, Issue 2, June, 1991.

4. Commercial International Security Requirements (CISR), Cutler, K. and Jones, F., Final Draft, September 9, 1991.

5. Computers at Risk - Safe Computing in the Information Age, National Research Council, National Academy Press, 1991.

6. Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 2: Authentication Framework, Draft International Standard DIS 10181-2, International Organization for Standardization, 13 May 1991

7. Assessing Federal and Commercial Information Security Needs, Ferraiolo, D., Gilbert, D., and Lynch, N., NIST Draft Internal Report, September 1992.

8. Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, Willis Ware, Editor, R-609-1, 1970, Reissued October 1979.

9. Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture, International Standard ISO 7498-2, International Organization for Standardization, 1988

10. Minimum Security Requirements for Multi-User Operating Systems: A Protection Profile for the U.S. Information Security Standard, National Institute of Standards and Technology, 1992 draft.

11. U.S. Information Technology Security Standard.

12. Role-Based Access Controls, Ferraiolo, D. and Kuhn, R., 15th National Computer Security Conference, October 1992.

13. A Comparison of Commercial and Military Computer Security Policies, IEEE Symposium on Computer Security and Privacy, April 1987.

DRAFT

LABEL BASED PROTECTION

FOR

MULTI-USER INFORMATION SYSTEMS

LEVEL 1

(LP-1)

A Protection Profile
Derived from the Federal Criteria for IT Security

Version 1.0

December 1992

Supersedes the
Trusted Computer System Evaluation Criteria
Class B1

DRAFT

LABEL-BASED PROTECTION - 1 (LP-1)

This Protection Profile has been developed to define a set of technical measures that can be incorporated into remote-access, resource- and information-sharing Information Technology (IT) products that will be used to protect two or more compartments of National Security Information classified according to US Executive Order 12356 (EO 12356). This profile can also be used to protect any information that has been designated as sensitive information for which information separation and access are based on sensitivity markings applied to the information.

Compliant IT products will provide protection for a compartmented information processing environment with which an organization can construct an automated information system to enhance or optimize the organization's ability to perform its mission.

In LP-1 conformant systems, the TCB is based on a multi-level security policy model for confidentiality that requires both discretionary and non-discretionary access controls. In relation to lower levels of protection functionality, LP-1 conformat systems have the following additional features.

a. Access control enforcement includes a defined subset of subjects and objects in the ADP system.

b. An informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects is included.

c. The supported labels accurately represent the sensitivity of objects and subjects, and are maintained on exported objects.

d. Any flaws identified by testing are removed or neutralized.

Cross References:

- Existing Criteria:
  (1) TCSEC: B1
  (2) ITSEC

  (3) CTCPEC

- Other Protection Profiles
  (1) TBD

COMPONENT SUMMARY:

LP-1 Functional Component Summary

Functional Component	Code & Level
Security Policy Support	
Accountability	
Identification & Authentication	I&A-2
System Entry	----
Trusted Path	----
Audit	AD-1
Access Control	AC-2
Discretionary	AC-2
Non-Discretionary	AC-2
Covert Channel Handling	-----
Availability	----
Resource Allocation	----
Fault Tolerance	----
Security Mgmt.	----
Reference Mediation	RM-1
TCB Logical Protection	P-1
TCB Physical Protection	----
TCB Self-checking	SC-1
TCB Start-Up and Recovery	----
TCB Privileged Operation	----
TCB Ease-of-Use	----

LP-1 Assurance Component Summary

Assurance Component Summary	**T2**
Development Assurance Components	
Development Process	
TCB Property Definition	PD-2
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-1
TCB Modular Decomposition	----
TCB Structuring Support	SP-1
TCB Design Disciplines	----
TCB Implementation Support	----

Assurance Component Summary	T2
TCB Testing & Analysis	
Functional Testing	FT-1
Penetration Analysis	----
Covert Channel Analysis	----
Operational Support	
User's Security Guidance	UG-1
Administrative Guidance	AG-1
Trusted Generation	TG-1
Development Environment	
Life Cycle Definition	----
Configuration Management	----
Trusted Distribution	----
Development Evidence	
TCB Protection Properties	EPP-2
Product Development	EPD-1
Product Testing & Analysis	
Functional Testing	EFT-1
Penetration Analysis	----
Covert Channel Analysis	----
Product Support	EPS-1
Evaluation Assurance Components	
Testing	
Test Analysis	TA-1
Independent Testing	IT-1
Review	
Development Environment	----
Operational Support	OSR-1
Analysis	
Design	----
Implementation	----

RATIONALE

1. Information Protection Policy

It is anticipated that organizations wishing to process compartmented-mode classified information will want to use IT products that are compliant with this profile in their automated information processing systems. These organizations should be able to trust the profile-compliant IT product to contribute to the protection of the compartmented information at least as much as they trust the properly cleared personnel who are using and managing the system.

2. Protection Philosophy

This profile presumes an environment providing control of access to shared resources both (1) on the basis of attributes that are controlled by the ordinary users of the system and (2) on the basis of attributes that are controlled only by the system administrators.

Profile compliant IT products will minimally meet the following objectives:

a. Enforce an informally defined security policy that describes the rules for accessing and administering access controls.
b. Associate explicit sensitivity labels with a defined subset of the system entities. Associate explicit sensitivity labels with each port through which information may be exported from or imported to the system. Maintain the accuracy of the access control labels as information moves within the system and through the ports.
c. Authenticate the claimed identity of each external human user of the IT product prior to establishing any internal entity to act on behalf of that user and firmly bind the authenticated user identity to the internal entity.
d. Selectively keep and protect a log of all actions or events that could affect system security so that they can be accurately attributed to the known user or system entity responsible for causing the action or event.

3. Expected Threats

The requirements for profile conforming IT products assume that these products are being used in an environment where there are multiple categories of classified data and users. A conforming IT product can be expected to protect the confidentiality of information in an environment where there are two or more levels of classified data and two or more levels of cleared users, but where malicious applications programs (e.g., Trojan Horses) and users are not present.

4. Assumed Environment

4.1 Characteristics

IT products complying with the requirements set forth in this profile are expected to be used in an environment with the following characteristics:

a. Multiple users will be accessing the operating system at the same time.
b. The IT product hardware base (e.g., CPU, printers, terminals, etc.) is protected from unauthorized physical access.
c. One or more administrators are assigned to manage the system in which the IT product is incorporated, including the security of the information it contains.
d. A need to control user access to objects exists and is based on an explicit sensitivity marking associated with the information (e.g, Confidential, Secret or Top Secret) and on that user's identity and membership in organizations or groups.
e. The IT product provides facilities for some or all of the authorized users to create programs that use the applications programming interface (API) and make those programs available to other users.
f. The IT product is used to provide a cooperative environment for the users to accomplish some task or group of tasks.

4.2 Environment Dependencies

Secure installation and operation of a product satisfying these profile requirements depends on provision of a number of elements in the installation environment. These include:

a. Physical security must be provided.
b. Cabling to other devices must be shown to be consistent with policy implemented by the product. For example, a “port” in the product is required to have an assigned label. No device can be connected to the port unless it has been established externally that the device is allowed to receive data with the same label.
c. Personnel allowed to access data processed by the installed product must already be authorized for such access.

5. Intended Use

Conforming IT products are useful in both general-purpose office automation environments with multiple data sensitivities and in specialized computing, network and mission environments. Examples of the office automation environment might include military headquarters and highly competitive procurement offices. An example of the specialized mission environment might be as a platform for a portable battlefield map and mission management application.

FUNCTIONAL REQUIREMENTS

I&A-2 Identification, Authentication, and Authorization

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2. The TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the ***clearance and authorization of individual users.*** These data shall be used by the TCB to authenticate the user's identity and to ensure ***that the subject security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user).***

3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user.

AD-1 - Minimal Audit

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

2. The TCB shall be able to record the following types of events:

- use of the identification and authentication mechanisms;

- introduction of objects into a user's address space (e.g., file open, program initiation), and deletion of objects;

- actions taken by computer operators and system administrators and/or system security officers.

The TCB shall be able to record any override of human-readable output markings.

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and the ***object security level.***

4. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or ***object security level***.

AC-2 Basic Access Control

1. Definition of Access Control Attributes

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined groups or both. Object attributes shall include defined access rights (e.g., read, write, execute) that can be assigned to subject attributes. ***Access control attributes corresponding to each individual policy shall be identified.***

Sensitivity labels associated with each subject and object shall be maintained by the TCB. The sensitivity labels shall be used as the basis for mandatory access control decisions.

The subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels.

The subject and object attributes shall accurately reflect the sensitivity and integrity of the subject or object. ***When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.***

2. Administration of Access Control Attributes

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects. The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users. These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. These controls shall be capable of including or excluding access to the granularity of a single user.

The rules for assignment and modification of access control attributes shall include those for attribute assignment to objects during import and export operations.

Export of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

1. Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

2. Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3. Labeling Human-Readable Output

The system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

Import of Non-labeled Data

In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

The authorization rules for the mandatory access control policy shall include:

The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). The following requirements shall hold for all accesses between all subjects and objects controlled by the TCB: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non- hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

The scope of the authorization rules shall include a defined subset of the product's subjects and objects and associated access control attributes. The coverage of authorization rules shall specify the types of objects and subjects to which these rules apply. If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

The authorization rules for each policy shall be defined separately. The TCB shall define and enforce the composition of policies, including the enforcement of the authorization rules (e.g., subject and object type coverage, enforcement precedence).

4. Subject and Object Creation and Destruction

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

RM-1 Mediation of References to a Defined Subject/Object Subset

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.

2. Reference mediation shall include references to the defined subset of subjects, objects, and resources protected under the TCB security policy, and to their policy attributes (***i.e., access rights, security levels***).

3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

P-1 Basic TCB Isolation

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Noncircumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

SC-1 Minimal Self Checking

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

ASSURANCES

Requirements for TCB Property Definition

PD-2 Informal Property Identification

The developer shall provide informal models for the functional components and sub-components of the profile. At a minimum, an informal model of the access control components shall be provided. Each informal model shall include (abstract) data structures and operations defining each functional component or sub-component, and a description of the model properties. The developer shall interpret (e.g., trace) the informal models within the product TCB. For each model entity, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that entity; (2) define the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the model properties. The developer's interpretation of each informal model, which defines the TCB properties, shall identify all TCB elements that do not correspond to any model entity and shall explain why these elements do not render the TCB properties invalid.

For the components that are not informally modeled, the developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement. The developer's interpretation of each functional requirement, which describes the TCB properties, shall identify all TCB elements that do not correspond to any functional requirement and shall explain why these elements do not render the TCB properties invalid.

Requirements for TCB Element Identification

ID-2: TCB Element Justification

The developer shall identify the TCB elements (i.e., software, hardware/firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).

The developer shall justify the protection relevance of the identified elements (i.e., only elements that can affect the correct operation of the protection functions shall be included in the TCB).

Requirements for TCB Interface Definition

IF-1: Interface Description

The developer shall describe all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB. The description shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.

The developer shall identify all call conventions (e.g., parameter order, call sequence requirements) and exceptions signaled at the TCB interface.

Requirements for TCB Structuring Support

SP-1: Process Isolation

The TCB shall maintain process isolation.

Requirements for Developer Functional Testing

FT-1: Conformance Testing

The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description.

The developer shall correct all flaws discovered by testing and shall retest the TCB until the protection functions are shown to work as claimed.

Requirements for User Guidance

UG-1: Users' Guide

The developer shall provide a User Guide which describes all protection services provided and enforced by the TCB. The User Guide shall describe the interaction between these services and provide examples of their use. The User Guide may be in the form of a summary, chapter or manual. The User Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

Requirements for Administrative Guidance

AG-1: Basic Administrative Guidance

The developer shall provide a Trusted Facility Manual intended for the product administrators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB. The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy. The Trusted Facility Manual shall explain the privileges and functions of administrators. The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.

Requirements for Trusted Generation

TG-1: Basic Trusted Generation

The developer shall establish and document the procedures that a consumer must perform to generate an operational TCB from the delivered copy of the master TCB. The consumer documentation shall identify any system parameters, which are initialized or set during system generation, that affect the TCB's conformance to the protection profile and state the acceptable ranges of values for those parameters.

Requirements for Evidence of TCB Protection Properties

EPP-2 Evidence of Informal Model Interpretation in the TCB

The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. The developer shall also provide an informal access control model and its interpretation within the TCB. The TCB properties, which are defined by this correspondence, shall be explained in this documentation.

Requirements for Evidence of Product Development

EPD-1: Description Of The TCB External Interface

The developer shall provide an accurate description of the functions, effects, exceptions and error messages visible at the TCB interface.

The developer shall provide a list of the TCB elements (hardware, software, and firmware).

Requirements for Evidence of Functional Testing

EFT-1: Evidence of Conformance Testing

The developer shall provide evidence of the functional testing that includes the test plan, the test procedures and the results of the functional testing.

Requirements for Evidence of Product Support

EPS-1: Evidence of Basic Product Support

The developer shall provide evidence that describes the policies, procedures, and plans established by the developer to satisfy the Operational Support and Development Environment requirements of the protection profile.

Requirements for Test Analysis

TA-1: ElementaryTest Analysis

The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results. The evaluator shall determine whether the product's protection properties, as described in the product documentation have been tested. The evaluator shall assess testing results to determine whether the product’s TCB works as claimed.

Requirements for Independent Testing

T-1: Elementary Independent Testing

A tester, independent of the producer or evaluator, shall perform functional and elementary penetration testing. This testing shall be based on the product's user and administrative documentation, and on relevant known penetration flaws. Satisfactory completion consists of demonstrating that all user-visible security enforcing functions and security-relevant functions work as described in the product's user and administrative documentation and that no discrepancies exist between the documentation and the product. Test results of the producer shall be confirmed by the results of independent testing. The evaluator may selectively reconfirm any test result.

If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results. The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results. The evaluator shall confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.

Requirements for Operational Support Review

OSR-1 Elementary Operational Support Review

The evaluator shall review all documentation focused on the activities of product use (e.g., Users Manuals) and product administration including installation, operation, maintenance, and trusted recovery (e.g., Trusted Facility Management Manuals). This review shall assess the clarity of presentation, difficulty in locating topics of interest, ease of understanding, and completeness of coverage. The need for separate manuals dedicated to protection-relevant aspects of the product should be assessed for effectiveness.

LABEL BASED PROTECTION

FOR

MULTI-USER INFORMATION SYSTEMS

LEVEL 2

(LP-2)

A Protection Profile
Derived from the Federal Criteria for IT Security

Version 1.0

December 1992

This document is undergoing review and
is subject to modification or withdrawal.
The contents of this document should not
be referenced in other publications.

Supersedes the
Trusted Computer System Evaluation Criteria
Class B2

LABEL-BASED PROTECTION - 2 (LP-2)

This Protection Profile has been developed to define a set of technical measures that can be incorporated into remote-access, resource- and information-sharing Information Technology (IT) products that will be used to protect up to three levels or more than two categories of National Security Information classified according to US Executive Order 12356 (EO 12356). This profile can also be used to protect any information that has been designated as sensitive information for which information separation and access are based on sensitivity markings applied to the information.

Compliant IT products will provide structured protection for a multi-level information processing environment with which an organization can construct an automated information system to enhance or optimize the organization's ability to perform its mission.

In LP-2 conformant systems, the TCB is based on a clearly defined and documented formal security policy model for confidentiality that requires both discretionary and non-discretionary access controls. Also, The TCB is relatively resistant to penetration. In relation to lower levels of protection functionality, LP-2 conformat systems have the following additional features.

a. Access control enforcement is extended to all subjects and objects in the ADP system.

b. Covert storage channels are identified and handled.

c. The TCB is modularized and carefully structured into protection-critical and non-protection-critical.

d. The TCB interface is well-defined and the TCB design and implementation enables it to be subjected to thorough testing and review. Penetration testing is also performed, and the TCB must be found relatively resistant to penetration.

e. Authentication mechanisms cover all policy attributes of a user (e.g., groups, secrecy and/or integrity levels, roles), not just the individual identity.

f. Security management is enhanced by the separation of system administrator and operator functions.

g. Configuration management controls are imposed.

Cross References:

- Existing Criteria:
  (1) TCSEC: B2
  (2) ITSEC
  (3) CTCPEC
- Other Protection Profiles
  (1) TBD

COMPONENT SUMMARY:

LP-2 Functional Component Summary

Functional Component	Code & Level
Security Policy Support	
Accountability	
Identification & Authentication	I&A-2
System Entry	----
Trusted Path	TP-1
Audit	AD-1
Access Control	AC-3
Discretionary	AC-3
Non-Discretionary	AC-3
Covert Channel Handling	CCH-2
Availability	----
Resource Allocation	----
Fault Tolerance	----
Security Mgmt.	SM-1+
Reference Mediation	RM-3
TCB Logical Protection	P-2
TCB Physical Protection	----
TCB Self-checking	SC-1
TCB Start-Up and Recovery	----
TCB Privileged Operation	PO-2
TCB Ease-of-Use	----

LP-2 Assurance Component Summary

Assurance Component Summary	**T5**
Development Assurance Components	
Development Process	
TCB Property Definition	PD-3
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-2
TCB Modular Decomposition	MD-2
TCB Structuring Support	SP-2
TCB Design Disciplines	----
TCB Implementation Support	IM-3

Assurance Component Summary	T5
TCB Testing & Analysis	
Functional Testing	FT-3
Penetration Analysis	PA-2
Covert Channel Analysis	CCA-1
Operational Support	
User's Security Guidance	UG-1
Administrative Guidance	AG-3
Trusted Generation	TG-2
Development Environment	
Life Cycle Definition	LC-2
Configuration Management	CM-2
Trusted Distribution	----
Development Evidence	
TCB Protection Properties	EPP-3
Product Development	EPD-3
Product Testing & Analysis	
Functional Testing	EFT-3
Penetration Analysis	EPA-2
Covert Channel Analysis	ECC-1
Product Support	EPS-2
Evaluation Assurance Components	
Testing	
Test Analysis	TA-4
Independent Testing	IT-3
Review	
Development Environment	DER-2
Operational Support	OSR-2
Analysis	
Design	DA-2
Implementation	CI-1

RATIONALE

6. Information Protection Policy

It is anticipated that organizations wishing to process either one level with three or more categories or one to three levels with one category of classified information will want to use IT products that are compliant with this profile in their automated information processing systems. These organizations should be able to trust the profile-compliant IT product to contribute to the protection of the classified information at least as much as they trust the properly cleared personnel who are using and managing the system.

7. Protection Philosophy

This profile presumes a hostile environment with divided, aggressive users. It provides control of access to shared resources both (1) on the basis of attributes that are controlled by the ordinary users of the system and (2) on the basis of attributes that are controlled only by the system administrators.

Profile compliant IT products will minimally meet the following objectives:

a. Enforce a formally defined security policy that describes the rules for controlling access to system subjects and objects. Use the access control rules to enforce an information flow policy that aims to control the use of covert storage channels.

b. Associate explicit sensitivity labels with each subject and object in the system. Associate explicit sensitivity labels with each port through which information may be exported from or imported to the system. Maintain the accuracy of the sensitivity labels as information moves within the system and through the ports.

c. Authenticate the claimed identity of each external human user of the IT product prior to establishing any internal entity to act on behalf of that user and firmly bind the authenticated user identity to the internal entity.

d. Selectively keep and protect a log of all actions or events (including use of covert storage channels) that could affect system security so that they can be accurately attributed to the known user or system entity responsible for causing the action or event.

e. Contains hardware and software mechanisms that can be independently evaluated to provide sufficient assurance that the system satisfies the previous four objectives.

f. Implements the enforcement of objectives in such a fashion that the enforcing mechanisms are protected from tampering and unauthorized changes by the entities these mechanisms are supposed to control.

8. Expected Threats

The requirements for profile conforming IT products assume that these products are being used in an environment where there are different levels or categories of classified data and users of differing clearance levels. A conforming IT product can be expected to protect the confidentiality of information in an environment where there are two levels or categories of classified data and two or more levels of cleared users and where there are collaborating, malicious users and software at each clearance level.

9. Assumed Environment

9.1 Characteristics

IT products complying with the requirements set forth in this profile are expected to be used in an environment with the following characteristics:

a. Multiple users will be accessing the operating system at the same time.

b. The IT product hardware base (e.g., CPU, printers, terminals, etc.) is protected from unauthorized physical access.

c. One or more administrators are assigned to manage the system in which the IT product is incorporated, including the security of the information it contains.

d. A need to control user access to information exists and is based on an explicit sensitivity marking associated with the information (e.g, Secret or Top Secret).

e. A need to control user access to all subjects and objects exists and is based on that user's identity and membership in organizations or groups.

f. The IT product provides facilities for some or all of the authorized users to create programs that use the applications programming interface (API) and make those programs available to other users.
g. The IT product is used to provide a cooperative environment for the users to accomplish some task or group of tasks.

9.2 Environment Dependencies

Secure installation and operation of a product satisfying these profile requirements depends on provision of a number of elements in the installation environment. These include:

a. Physical security must be provided.
b. Cabling to other devices must be shown to be consistent with policy implemented by the product. For example, a “port” in the product is required to have an assigned label. No device can be connected to the port unless it has been established externally that the device is allowed to receive data with the same label.
c. Personnel allowed to access data processed by the installed product must already be authorized for such access.

10. Intended Use

Conforming IT products are useful in both general-purpose office automation environments with multiple data sensitivities (or “classifications”) and multiple levels of user authorizations (or “clearances”) and in specialized computing, network and mission environments. Examples of the office automation environment might include military headquarters and highly competitive procurement offices. Examples of the network environments include use as the basis for a multilevel secure network management center or a trusted guard gateway operating between two networks processing different levels of information. An example of the specialized mission environment might be as a platform for a portable battlefield map and mission management application.

FUNCTIONAL REQUIREMENTS

I&A-2 Identification, Authentication, and Authorization

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2. The TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the *clearance and authorization of individual users.* These data shall be used by the TCB to authenticate the user's identity and to ensure *that the subject security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user).*

3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user.

TP-1 Login Trusted Path

The TCB shall support a trusted communication path between itself and the user for initial identification and authentication. Communications via this path shall be initiated exclusively by a user.

AD-1 - Minimal Audit

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

2. The TCB shall be able to record the following types of events:

- use of the identification and authentication mechanisms;
- introduction of objects into a user's address space (e.g., file open, program initiation), and deletion of objects;
- actions taken by computer operators and system administrators and/or system security officers.

The TCB shall be able to record any override of human-readable output markings. ***The TCB shall also be able to audit the identified event that may be used in the exploitation of covert channels.***

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and the *object security level.*

4. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or *object security level.*

AC-3 Extended Access Control

1. Definition of Access Control Attributes

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined groups or both. Object attributes shall include defined access rights (e.g., read, write, execute) that can be assigned to subject attributes. *Access control attributes corresponding to each individual policy shall be identified.*

*Sensitivity labels associated with each subject and **storage object that is directly or indirectly accessible by subjects external to the TCB** shall be maintained by the TCB. The sensitivity labels shall be used as the basis for mandatory access control decisions.*

The subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels.

The subject and object attributes shall accurately reflect the sensitivity and integrity of the subject or object. *When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.*

The TCB shall immediately notify a terminal user of each ***change in the security level associated with that user during an interactive session.*** A terminal user shall be able to query the TCB as desired for a display of the subject's complete ***sensitivity label****.*

The TCB shall support the assignment of ***minimum and maximum security levels*** to all attached physical devices. These ***security levels*** shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

2. Administration of Access Control Attributes

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects. The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users. These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. These controls shall be capable of including or excluding access to the granularity of a single user.

The rules for assignment and modification of access control attributes shall include those for attribute assignment to objects during import and export operations.

Export of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

1. Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

2. Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3. Labeling Human-Readable Output

The system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

Import of Non-labeled Data

In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

The scope of the authorization rules shall include all subjects, storage objects (e.g., processes, segments, devices) and associated access control attributes that are directly or indirectly accessible to subjects external to the TCB. The scope of the authorization rules shall ***also include all policy and status attributes of subjects and storage objects (e.g., quotas, object existence, size, access time, creation and modification time, locked/ unlocked).*** If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

The authorization rules for the mandatory access control policy shall include:

The TCB shall enforce a mandatory access control policy over all ***resources (i.e., subjects, storage objects, and I/O devices that are directly or indirectly accessible by subjects external to the TCB.*** *The following requirements shall hold for all accesses between all subjects* ***external to the TCB and all objects directly or indirectly accessible by these subjects:*** *A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non- hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.*

The authorization rules for each policy shall be defined separately. The TCB shall define and enforce the composition of policies, including the enforcement of the authorization rules (e.g., subject and object type coverage, enforcement precedence).

4. Subject and Object Creation and Destruction

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

CCH-2 Storage Channel Audit and Bandwidth Limitation

1. The TCB and privileged applications shall include functions that help audit the use of covert storage channels. These functions shall enable the identification of the transmitter, receiver, and specific covert channels used (e.g., TCB and privileged application element used to transmit information). TCB functions that help limit the bandwidth and/or eliminate covert storage channels shall also be provided. The bandwidth limits for each channel shall be settable by system administrators.

2. The functions added to the TCB and privileged applications for storage channel auditing shall be identified for each channel and shall be available in common product configurations. If audit functions are not added to certain storage channels (e.g., hardware storage channels), evidence must be provided to justify why these channels do not represent a security threat for the intended use of the product. TCB and privileged application functions that help limit the bandwidth and/or eliminate covert storage channels shall also be available in common product configurations.

If channel bandwidth limitation and channel elimination functions are not added to certain storage channels (e.g., hardware storage channels), evidence must be provided to justify why these channels do not represent a security threat for the intended use of the product.

SM-1 Minimal Security Management

1. The TCB shall provide an installation mechanism for the setting and updating of its configuration parameters, and for the initialization of its protection-relevant data structures before any user or administrator policy attributes are defined. It shall allow the configuration of TCB internal databases and tables.

2. The TCB shall provide protected mechanisms for displaying and modifying the security policy parameters.

3. The TCB shall provide protected mechanisms for manually displaying, modifying, or deleting user registration and account parameters. These parameters shall include unique user identifiers, their account, and their associated user name and affiliation. The TCB shall allow the manual enabling and disabling of user identities and/or accounts.

4. ***The TCB shall support separate operator and administrator functions. The operator functions shall be restricted to those necessary for performing routine operations. The operator functions*** shall allow the enabling and disabling of peripheral devices, mounting removable storage media, backing-up and recovering user objects; maintaining the TCB hardware and software elements (e.g., on-site testing); and starting and shutting down the system. **[SM-3]**

5. The use of the protected mechanisms for system administration shall be limited to authorized administrative users.

RM-3 Mediation of References to Subject and Object Attributes

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.

2. Reference mediation shall include control of references to all subjects, objects, and resources protected under the TCB security policy, to their policy (***i.e., access rights, security levels***) and status attributes (e.g., existence, length, locking state).

3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

P-2 TCB Isolation and Consistency

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Non-circumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

TCB protection shall also maintain the consistency of TCB global variables and eliminate undesirable dependencies of the TCB on unprivileged subject or user actions.

3. Consistency of TCB global variables requires that consistency conditions defined over TCB internal variables, objects, and functions hold before and after any TCB invocation.

4. Elimination of undesirable dependencies of the TCB on unprivileged subject actions requires that any TCB invocation by an unprivileged subject (or user) input to a TCB call may not place the TCB in a state such that it is unable to respond to communication initiated by other users.

SC-1 Minimal Self Checking

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

PO-2 Privilege Association with TCB Modules

1. TCB privileges needed by individual functions, or groups of functions, of a functional component shall be identified. Privileged TCB calls or access to privileged TCB objects, such as user and group registration files, password files, security and integrity-level definition file, role definition file, audit-log file shall also be identified. It shall be possible to associate TCB privileges with TCB operations performed by administrative users.

2.The modules of a TCB function shall be associated only with the privileges necessary to complete their task.

3. Support for product privilege implementation and association with TCB modules provided by lower-level mechanisms or procedures (e.g., operating system, processors, language) shall be provided.

ASSURANCES

Requirements for TCB Property Definition

PD-3 Property Specification by Model Interpretation

The developer shall provide formal models for the functional components and sub-components of the profile. At a minimum, a formal model of the access control components shall be provided. The properties of the formal models shall be clearly stated. The developer shall provide an interpretation of the models in the DIS of the product's TCB. For each model entity, the developer shall: (1) identify the TCB elements and their DIS (if any) that implement that entity; (2) define the operation of these TCB elements, and (3) demonstrate, by coherent arguments, that the DIS of these elements is consistent with the model properties. The developer's interpretation of each formal model, which specifies the TCB properties, shall identify all TCB and DIS elements (if any) that do not correspond to any model entity and shall explain why these elements do not render the TCB properties invalid.

An informal model of reference mediation and TCB protection shall be provided. For the components that are not modeled, the developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement. The developer's interpretation of each functional requirement, which describes the TCB properties, shall include all the TCB elements.

Requirements for TCB Element Identification

ID-2: TCB Element Justification

The vendor shall identify the TCB elements (i.e., software, hardware/firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).

The developer shall justify the protection relevance of the identified elements (i.e., only elements that can affect the correct operation of the protection functions shall be included in the TCB). If protection-irrelevant elements are included in the TCB, the developer shall provide a rationale for such inclusion.

Requirements for TCB Interface Definition

IF-2: Interface Descriptive Specification

The developer shall define all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB.

The developer shall provide and maintain a descriptive interface specification (DIS) of the TCB that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. The DIS shall identify the TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions signaled. The DIS shall also include the TCB call identifier, parameter types (e.g., input, output), the effect of the call, TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions handled and signaled. It shall be shown to be an accurate description of the TCB interface.

The DIS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.

If the TCB consists of a kernel and privileged processes, the developer shall separately identify and define the interfaces for the kernel and each privileged process.

The TCB interface definition must also include all effects of a call including the direct visibility and alterability of internal TCB variables and functions.

Requirements for Modular Decomposition

MD-2: Module-level Decomposition

The developer shall design the TCB as a small number (e.g., 10 to 100) of design and implementation subsystems that have well-defined functional relationships and shared-data dependencies. The developer shall identify the specific TCB protection functions (if any) associated with each subsystem and the TCB interfaces (if any) implemented by each subsystem.

The developer shall design each subsystem as a set of modules. For each module, the developer shall describe: the role or purpose of the module, the set of related functions performed by the module, and the module interface (i.e., the set of invocable functions, calling conventions, parameters, global variables, and results). The developer shall identify the protection functions of, and describe the interfaces between, these modules. The developer shall choose the modules so that the set of functions implemented by the module, the module's contribution to the TCB protection properties, and the interface(s) to the module can be described concisely (e.g., the module shall have a single purpose). The TCB structuring into modules shall be based on well-defined module relationships; for example, the contains relation (e.g., A is part of B) or the “uses” relation (e.g., A is correct only if B is correct).

Requirements for TCB Structuring Support

SP-2: Support for Storage Objects

The TCB shall maintain process isolation. The TCB shall separate those elements that are protection-critical from those that are not. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate access-control attributes (e.g., readable, writable).

Requirements for Implementation Support

IM-3: Module Correspondence Support

The developer shall maintain engineering diagrams and source code (as applicable) for all TCB elements. The diagrams and source code for each module of the TCB shall be identified and provided as configuration items.

Requirements for Developer Functional Testing

FT-3: Specification-Driven TCB Interface Testing

The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description or specification. The tests shall exercise the boundary conditions of the protection functions. The developer shall generate the test conditions and data from the ***Descriptive Interface Specification(s)***. The developer test procedures shall include the tests used to demonstrate the absence of all flaws discovered in previous versions of the TCB.

The developer shall correct all flaws discovered by testing and shall retest the TCB to show that all discovered flaws have been eliminated, no new flaws have been introduced, and the protection functions work as claimed.

Requirements for Penetration Analysis

PA-2 Flaw-Hypothesis Testing

The developer shall define the TCB configuration, interface, and protection functions that are subject to penetration testing. For each test, the developer shall identify the goal of the test and the criteria for successful penetration. The developer shall illustrate how, in addition to system reference manuals and TCB interface description, the DIS, source code, and hardware and firmware specifications are used to define penetration-test conditions. For each test, the developer shall document all test conditions, data (e.g., test set-up, function call parameters, and test outcomes), and coverage.

The developer shall generate the test conditions from flaw-hypotheses derived by negating assertions of TCB design capabilities and by providing counter examples that show that these assertions are false. The developer shall confirm the flaw hypotheses by checking design and implementation documentation, by defining the test data and running test programs, or by referring to known classes of penetration flaws found in other TCBs. The refutation of any hypothesis shall be documented.

For each uncovered flaw, the developer shall define and document scenarios of flaw exploitation and shall identify all penetration outcomes resulting from that scenario. The cause of the flaw shall be identified and documented.

Requirements for Covert-Channel Analysis

CCA-1 Analysis of Covert Storage Channels

1. *Identification:* The developer shall identify all sources of information used in covert-storage-channel analysis. These sources shall include TCB reference manuals and DIS. The developer shall define the identification method used. The developer shall demonstrate that the chosen identification method is sound (e.g., it leads to the discovery of all covert storage channels in the DIS or source documentation) and repeatable (i.e., independent evaluators can use the method on the same sources of covert-storage-channel information and can obtain the same results.) The developer shall define scenarios of use for each covert storage channel.

2. *Bandwidth Measurement or Engineering Estimation:* The developer shall define the method used for covert-storage-channel bandwidth estimation. In measuring TCB performance for covert-channel-bandwidth estimation, the developer shall satisfy the following assumptions. The maximum bandwidth estimation shall be based on the assumptions that the storage channel is noiseless, that the senders and receivers are not delayed by the presence of other processes in the product, and that the sender-receiver synchronization time is negligible. The choice of informal estimation methods shall define and justify the coding method and, therefore, the distribution of “0s” and “1s” in all transmissions.

The developer shall select TCB primitives to be measured for bandwidth determination from real scenarios of covert-storage-channel use. The developer shall specify TCB measurement environment for the bandwidth measurements. This specification shall include: (1) the speed of the product functions, (2) the product configuration, (3) the sizes of the memory and cache components, and (4) the product initialization. The sensitivity of the measurement results to configuration changes shall be documented. The covert-storage-channel measurements shall include the fastest TCB function calls for altering, viewing, and setting up the transmission environment; the demonstrably fastest process (context) switch time shall also be included in the bandwidth measurements. All measurements shall be repeatable.

3. *Covert Channel Testing:* The developer shall test all the use of all identified covert storage channels to determine whether the handling functions work as intended.

Requirements for User Guidance

UG-1: Users' Guide

The developer shall provide a User Guide which describes all protection services provided and enforced by the TCB. The User Guide shall describe the interaction between these services and provide examples of their use. The User Guide may be in the form of a summary, chapter or manual. The User Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

Requirements for Administrative Guidance

AG-2: Detailed Administrative Guidance

The developer shall provide a Trusted Facility Manual intended for the product administrators and operators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The T

Requirements for Evidence of TCB Protection Properties

EPP-3 Evidence of Formal Model Interpretation in the DIS

The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. This documentation shall describe how the TCB implements the reference monitor concept. The developer shall also provide a formal access-control model and an informal reference mediation and TCB protection model. The TCB properties, which are defined by this correspondence and the interpretation of these models within the DIS of the TCB shall be documented by the product developer.

Requirements for Evidence of Product Development

EPD-3: Analysis Of The TCB External Interface

The developer shall provide TCB Design Specifications that include: a list of the TCB elements (hardware, software, and firmware configuration items); a list of protection services provided to the TCB by hardware, software, and firmware that is not part of the TCB; an explanation of the techniques and criteria used during the modular decomposition of the TCB; a description of the policy allocations, functions, and interactions among the major TCB subsystems; and module level descriptions of all software and hardware in the TCB.

The developer shall provide a Descriptive Interface Specification (DIS) that describes the functions, effects, exceptions and error messages visible at the TCB interface. The developer shall show that the DIS is an accurate representation of the TCB's external interfaces.

The developer shall provide TCB Implementation Data consisting of the engineering diagrams for all hardware included in the TCB and the source code used to generate the TCB software and firmware.

Requirements for Evidence of Functional Testing

EFT-3: Evidence of Specification-Driven Testing

The developer shall provide evidence of the functional testing that includes the test plan, the test procedures, and the results of the functional testing. The test, plans, procedures, and results shall be maintained under the same configuration control as the TCB software. The test plans shall identify the TCB specification used in the derivation of the test conditions, data, and coverage analysis.

Requirements for Evidence of Penetration Analysis

EPA-2: Evidence of Flaw-Hypothesis Generation and Testing

The developer shall provide evidence of penetration testing. The penetration evidence shall identify all product documentation and development evidence on which the search for flaws was based. The penetration evidence shall describe the scenarios for exploiting each potential flaw in the system and the penetration test conditions, data (e.g., test set-up, function call parameters, and test outcomes), coverage, and conclusions derived from each scenario. The penetration evidence shall summarize both refuted and confirmed flaws hypothesis.

Requirements for Evidence of Covert Channel Analysis

ECC-1: Evidence of Covert Storage Channel Analysis and Handling

The developer's documentation shall present the results of the covert-storage-channel analysis and the trade-offs involved in restricting these channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The developer shall provide the bandwidths of known covert-storage-channels whose use is not detectable by the auditing mechanism. The documentation of each identified storage channel shall consist of the variable that can be viewed/altered by the channel and the TCB interface functions that can alter or view that variable. The measurements of each TCB function call used by covert-storage channels must be documented and the bandwidth computation shall be included for each channel. The measurement environment should be documented as specified. Test documentation shall include results of testing the effectiveness of the methods used to reduce covert-storage-channel bandwidths**.**

Requirements for Evidence of Product Support

EPS-2: Evidence of Defined Product Support

The developer shall provide documentation that defines the policies, procedures, plans, and tools established by the developer to satisfy the Operational Support and Development Environment requirements of the protection profile.

Requirements for Test Analysis

TA-4: Comprehensive Test Analysis

The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and penetration analysis, and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results, and general correctness (e.g., defect trend from regression testing). This analysis shall examine the testability of requirements, the adequacy of the tests to measure the required properties, the deviation of the actual results obtained from the expected results. The analysis shall extend to trace all defects identified, corrected, and retested. The analysis shall include an assessment of test coverage and completeness, and defect frequency. The results of testing shall be interpreted in terms that express product performance and protection adequacy. The evaluator shall determine whether the product's protection properties, as defined for all protection-relevant modules of the TCB, and all relevant known penetration flaws have been tested. The evaluator shall independently develop, test, and document additional flaw hypotheses. The evaluator shall assess testing results to determine whether the product's TCB works as claimed, that the TCB's implementation is consistent with the DIS, and whether there are any obvious ways (i.e., ways that are known, or that are readily apparent or easily discovered in product documentation) for an unauthorized user to bypass the policy implemented by the TCB or otherwise defeat the product's TCB, and whether all discovered TCB flaws have been corrected and no new TCB flaws introduced. No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. ***The testing results shall show that the methods used to reduce covert channel bandwidths have been effective for all evaluated configurations.*** The evaluator shall determine whether the product is relatively resistant to penetrations.

Requirements for Independent Testing

IT-3: Comprehensive Independent Testing.

The evaluator shall independently perform functional and elementary penetration testing to confirm test results. This testing may be selective and shall be based on (1) the results of other independent and/or producer testing, (2) the TCB's DIS, (3) other product design and implementation documentation, (4) the product's user and administrative documentation, (5) relevant known penetration flaws**,** and (6) evaluator-developed TCB penetration flaw hypotheses and corresponding tests that attempt to exploit the hypothesized flaws. Satisfactory completion consists of demonstrating that all TCB functions work as described in the product's relevant documentation, that test results are consistent, and that no discrepancies exist between the documentation and the product. Satisfactory penetration test completion shall be determined by the subjective judgement (which may be supported algorithmically) of the evaluator. Test duration agreements may further constrain this judgement. Categorization of an actual penetration flaw shall be based on the reproducibility of that flaw. Flaws that are discovered, but are not reproducible shall remain categorized as potential penetration flaws. All actual penetration flaws must be corrected and retested.

The evaluator shall provide a penetration test plan document that describes the additional evaluator-developed flaw hypotheses and associated tests. The evaluator shall execute these tests and shall report any discovered flaws to the producer as part of the testing results. At the conclusion of penetration testing, the evaluator shall provide copies of this penetration test plan and its test results to the producer. The producer shall ensure that this test plan and its test results are incorporated into the rest of the product's testing documentation and that such documentation is available for further analysis throughout the life of the product.

The evaluator shall test for covert channel bandwidth reductions to determine the effectiveness of handling method(s) in reducing the bandwidths of identified covert channels for all evaluated configurations.

If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results. The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results. The evaluator shall also confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.

Requirements for Development Environment

DER-2: Enhanced Development Environment Review

The evaluator shall review the producer's development and maintenance process description documentation and shall conduct a random audit of the producer's processes using the evidence generated by each process to determine the degree of discipline enforced upon and within the process, and to determine the protection characteristics associated with the product's development and maintenance. The results of this review shall establish, for the evaluator, the producer's development environment, its policies, and the degree of enforcement maintained during development execution. The results of this review shall also confirm the producer's general conformance with relevant development environment requirements**.**

Requirements for Operational Support

OSR-2 Enhanced Operational Support Review

The evaluator shall review all documentation focused on the activities of product use (e.g., Users Manuals) and product administration including installation, operation, maintenance, and trusted recovery (e.g., Trusted Facility Management Manuals). This review shall assess the clarity of presentation, difficulty in locating topics of interest, ease of understanding, and completeness of coverage. The need for separate manuals dedicated to

> protection-relevant aspects of the product should be assessed for effectiveness. The evaluator shall randomly select a sample of the documented protection-relevant features and procedures and execute them to determine if their descriptions are accurate and correct.

Requirements for Design Analysis

DA-2: Enhanced Design Analysis

The evaluator shall determine whether the producer has performed the activities defined in the development process assurance requirements of the protection profile for TCB property definition and TCB design. The evaluator shall determine whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's activities for completeness, consistency, and correctness of design with respect to requirements.

Requirements for Implementation Analysis

CI-1: Elementary Implementation Analysis

> The evaluator shall conduct a code inspection on a small sample of randomly selected product code. The assessment shall focus on clarity of the coding style, adherence to coding standards, coding documentation, and on possible software defects that may be present with respect to the product’s informal design. The inspection shall be performed to obtain only a sample of possible software defects, not to capture all such possible defects. The evaluator shall report all discovered defects to the producer; the assessment shall report the number of defects found per line of code inspected from the random sample size. Use of producer-provided code inspection results can supplement this sample inspection. All trapdoors built into the product for maintenance purposes shall be identified by the producer and shown to be protected by the product.

DRAFT

LABEL BASED PROTECTION

FOR

MULTI-USER INFORMATION SYSTEMS

LEVEL 3

(LP-3)

A Protection Profile
Derived from the Federal Criteria for IT Security

Version 1.0

December 1992

This document is undergoing review and is subject to modification or withdrawal. The contents of this document should not be referenced in other publications.

Supersedes the
Trusted Computer System Evaluation Criteria
Class B3

DRAFT

LABEL-BASED PROTECTION - 3 (LP-3)

This Protection Profile has been developed to define a set of technical measures that can be incorporated into remote-access, resource- and information-sharing Information Technology (IT) products that will be used to protect up to three levels and multiple categories of National Security Information classified according to US Executive Order 12356 (EO 12356). This profile can also be used to protect any information that has been designated as sensitive information for which information separation and access are based on sensitivity markings applied to the information. This profile is intended for use in environments where the presence potentially malicious application software (e.g., Trojan Horses) mandate the use of high-assurance products.

Compliant IT products will provide highly-structured, conceptually simple protection mechanisms for a multi-level information processing environment with which an organization can construct an automated information system to enhance or optimize the organization's ability to perform its mission.

In LP-3 conformant systems, the TCB is demonstrably based on a clearly defined and documented formal security policy model (i.e., the interpretation of the policy model within the TCB is shown to be valid). The TCB is resistant to penetration. In relation to lower levels of protection functionality, LP-3 conformat systems have the following additional features.

- *a. The TCB must satisfy all requirements of the reference monitor concept (i.e., TCB protection, reference mediation, and TCB structuring and complexity minimization to enhance TCB verification; viz., Appendix B).*
- *b. Covert storage and timing channels are analyzed and handled.*
- *c. The TCB includes trusted recovery functions and a trusted path mechanism that includes general user commands, not just login commands.*
- *d. The audit mechanisms include alarms that signal accumulation of events representing potential security violations.*

e. *Security management is enhanced by the fine-grain separation of system administrator and operator functions and by the minimization of security irrelevant functions of security roles.*

f. *Stringent configuration management controls are imposed.*

g. *The TCB must be found resistant to penetration.*

Cross References:

- Existing Criteria:
  (1) TCSEC: B3
  (2) ITSEC
  (3) CTCPEC
- Other Protection Profiles
  (1) TBD

COMPONENT SUMMARY:

LP-3 Functional Component Summary

Functional Component	Code & Level
Security Policy Support	
Accountability	
Identification & Authentication	I&A-2
System Entry	----
Trusted Path	TP-2
Audit	AD-1+
Access Control	AC-3+
Discretionary	AC-3+
Non-Discretionary	AC-3
Covert Channel Handling	CCH-3
Availability	----
Resource Allocation	----
Fault Tolerance	----
Security Mgmt.	SM-1++
Reference Mediation	RM-3
TCB Logical Protection	P-3
TCB Physical Protection	----
TCB Self-checking	SC-1
TCB Start-Up and Recovery	TR-1
TCB Privileged Operation	PO-2
TCB Ease-of-Use	----

LP-3Assurance Component Summary

Assurance Component Summary	**T6**
Development Assurance Components	
Development Process	
TCB Property Definition	PD-3
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-2
TCB Modular Decomposition	MD-3
TCB Structuring Support	SP-3
TCB Design Disciplines	DD-2
TCB Implementation Support	IM-3

Assurance Component Summary	T6
TCB Testing & Analysis	
Functional Testing	FT-3
Penetration Analysis	PA-2
Covert Channel Analysis	CCA-2
Operational Support	
User's Security Guidance	UG-1
Administrative Guidance	AG-3
Trusted Generation	TG-3
Development Environment	
Life Cycle Definition	LC-3
Configuration Management	CM-3
Trusted Distribution	----
Development Evidence	
TCB Protection Properties	EPP-3
Product Development	EPD-4
Product Testing & Analysis	
Functional Testing	EFT-3
Penetration Analysis	EPA-2
Covert Channel Analysis	ECC-2
Product Support	EPS-3
Evaluation Assurance Components	
Testing	
Test Analysis	TA-4
Independent Testing	IT-3
Review	
Development Environment	DER-3
Operational Support	OSR-3
Analysis	
Design	DA-3
Implementation	CI-3

RATIONALE

11. Information Protection Policy

It is anticipated that organizations wishing to process two to three levels of classified information with multiple categories will want to use IT products that are compliant with this profile in their automated information processing systems. These organizations should be able to trust the profile-compliant IT product to contribute to the protection of the classified information at least as much as they trust the properly cleared personnel who are using and managing the system.

12. Protection Philosophy

This profile presumes a hostile environment with divided, aggressive users. It provides control of access to shared resources both (1) on the basis of attributes that are controlled by the ordinary users of the system and (2) on the basis of attributes that are controlled only by the system administrators.

Profile compliant IT products will minimally meet the following objectives:

a. Employ a reference validation mechanism to enforce a formally defined security policy that describes the rules for controlling access to system subjects and objects and use the access control rules to enforce an information flow policy that aims to control the use of covert storage and timing channels.

b. Associate explicit sensitivity labels with each subject and object in the system and each port through which information may be exported from or imported to the system. Maintain the accuracy of the sensitivity labels as information moves within the system and through the ports.

c. Authenticate the claimed identity of each external human user of the IT product prior to establishing any internal entity to act on behalf of that user and firmly bind the authenticated user identity to the internal entity.

d. Selectively keep and protect a log of all actions or events (including use of covert storage channels) that could affect system security so that they can be accurately attributed to the known user or system entity responsible for causing the action or event. Also, alert the system administrator when a series of events indicates an imminent violation of the security policy.

e. Contains hardware and software mechanisms that can be independently evaluated to provide sufficient assurance that the system satisfies the previous four objectives.
f. Implements the enforcement of objectives a through d in such a fashion that the enforcing mechanisms are protected from tampering and unauthorized changes by the information moving entities that the mechanisms are supposed to control.

13. Expected Threats

The requirements for profile conforming IT products assume that these products are being used in an environment where there are different levels and categories of classified data and users of differing clearance levels. A conforming IT product can be reasonably expected to protect the confidentiality of information in an environment where there are three levels and multiple categories of classified data, and two or more levels of cleared users and where there are collaborating, malicious users and software at each clearance level.

14. Assumed Environment

14.1 Characteristics

IT products complying with the requirements set forth in this profile are expected to be used in an environment with the following characteristics:

a. Multiple users will be accessing the operating system at the same time.
b. The IT product hardware base (e.g., CPU, printers, terminals, etc.) is protected from unauthorized physical access.
c. One or more personnel are assigned to manage the system in which the IT product is incorporated, including the security of the information it contains.
d. A need to control user access to information exists and is based on an explicit sensitivity marking associated with the information (e.g, Secret or Top Secret).
e. There is a need to control user access to information exists and is based on that user’s identity and membership in organizations or groups.

f. The IT product provides facilities for some or all of the authorized users to create programs that use the applications programming interface (API) and make those programs available to other users.

g. The IT product is used to provide a cooperative environment for the users to accomplish some task or group of tasks.

14.2 Environment Dependencies

Secure installation and operation of a product satisfying these profile requirements depends on provision of a number of elements in the installation environment. These include:

a. Physical security must be provided. For US Government classified operation, physical security equivalent to PP-2 would be required.

b. Cabling to other devices must be shown to be consistent with policy implemented by the product. For example, a “port” in the product is required to have an assigned label. No device can be connected to the port unless it has been established externally that the device is allowed to receive data with the same label.

c. Personnel allowed to access data processed by the installed product must already be authorized for such access.

15. Intended Use

Conforming IT products are useful in both general-purpose office automation environments with multiple data sensitivities (or “classifications”) and multiple levels of user authorizations (or “clearances”) and in specialized computing, network and mission environments. Examples of the office automation environment might include military headquarters and highly competitive procurement offices. Examples of the network environments include use as the basis for a multilevel secure network management center or a trusted guard gateway operating between two networks processing different levels of information. An example of the specialized mission environment might be as a platform for a portable battlefield map and mission management application.

FUNCTIONAL REQUIREMENTS

Requirements for Identification and Authentication

I&A-2 Identification, Authentication, and Authorization

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2. The TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the *clearance and authorization of individual users.* These data shall be used by the TCB to authenticate the user's identity and to ensure *that the subject security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user).*

3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user.

Requirements for Trusted Path

TP-2 Trusted User-to-TCB Communication

The TCB shall support a trusted communication path between itself and users for use whenever a positive user-to-TCB connection is required (e.g., login, change of policy attributes). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other communication paths.

Requirements for Audit

AD-1+ Minimal Audit

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

2. The TCB shall be able to record the following types of events:

- use of the identification and authentication mechanisms;

- introduction of objects into a user's address space (e.g., file open, program initiation), and deletion of objects;

- actions taken by computer operators and system administrators and/or system security officers.

The TCB shall be able to record any override of human-readable output markings. The TCB shall also be able to audit the identified event that may be used in the exploitation of covert channels.

The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of auditable events that may indicate an imminent violation of the product's security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded, and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event. [AD-3]

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and the *object security level.*

4. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or *object security level.*

Requirements for Access Control

AC-3 + Extended Access Control

1. Definition of Access Control Attributes

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined groups or both. Object attributes shall include defined access rights (e.g., read, write, execute) that can be assigned to subject attributes. *Access control attributes corresponding to each individual policy shall be identified.*

Sensitivity labels associated with each subject and storage object that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. The sensitivity labels shall be used as the basis for mandatory access control decisions.

The subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels.

The subject and object attributes shall accurately reflect the sensitivity and integrity of the subject or object. *When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.*

The TCB shall immediately notify a terminal user of each *change in the security level associated with that user during an interactive session.* A terminal user shall be able to query the TCB as desired for a display of the subject's complete *sensitivity label.*

The TCB shall support the assignment of *minimum and maximum security levels* to all attached physical devices. These *security levels* shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

2. Administration of Access Control Attributes

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects. The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users. These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. ***(i.e., these rules shall define the distribution, revocation, and review of access control attributes). The controls defined by these rules shall be capable of specifying for each named object, a list of individuals and a list of groups of named individuals, with their respective access rights to that object. Furthermore, for each named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is given [AC-4}.*** These controls shall be capable of including or excluding access to the granularity of a single user.

The rules for assignment and modification of access control attributes shall include those for attribute assignment to objects during import and export operations.

Export of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

1. Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

2. Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3. Labeling Human-Readable Output

The system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

Import of Non-labeled Data

In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

The scope of the authorization rules shall include all subjects, storage objects (e.g., processes, segments, devices) and associated access control attributes that are directly or indirectly accessible to subjects external to the TCB. The scope of the authorization rules shall *also include all policy and status attributes of subjects and storage objects (e.g., quotas, object existence, size, access time, creation and modification time, locked/unlocked).* If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

The authorization rules for the mandatory access control policy shall include:

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices that are directly or indirectly accessible by subjects external to the TCB. The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non- hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

The authorization rules for each policy shall be defined separately. The TCB shall define and enforce the composition of policies, including the enforcement of the authorization rules (e.g., subject and object type coverage, enforcement precedence).

4. Subject and Object Creation and Destruction

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

Requirements for Covert Channel Handling

CCH-3 Timing Channel Audit and Bandwidth Limitation

1. The TCB and privileged applications shall include functions that help audit the use of covert storage channels. These functions shall enable the identification of the transmitter, receiver, and specific covert channels used (e.g., TCB and privileged application element used to transmit information). TCB functions that help limit the bandwidth and/or eliminate covert storage channels shall also be provided. The bandwidth limits for each channel shall be settable by system administrators.

2. The functions added to the TCB and privileged applications for storage channel auditing shall be identified for each channel and shall be available in common product configurations. If audit functions are not added to certain storage channels (e.g., hardware storage channels), evidence must be provided to justify why these channels do not represent a security threat for the intended use of the product. TCB and privileged application functions that help limit the bandwidth and/or eliminate covert storage or timing channels shall also be available in common product configurations.

   If channel bandwidth limitation and channel elimination functions are not added to certain storage or timing channels (e.g., hardware channels), evidence must be provided to justify why these channels do not represent a security threat for the intended use of the product.

Requirements for Security Management

SM-1++ Minimal Security Management

1. The TCB shall provide an installation mechanism for the setting and updating of its configuration parameters, and for the initialization of its protection-relevant data structures before any user or administrator policy attributes are defined. It shall allow the configuration of TCB internal databases and tables.

2. The TCB shall provide protected mechanisms for displaying and modifying the security policy parameters.

3. The TCB shall provide protected mechanisms for manually displaying, modifying, or deleting user registration and account parameters. These parameters shall include unique user identifiers, their account, and their associated user name and affiliation. The TCB shall allow the manual enabling and disabling of user identities and/or accounts.

4. *The TCB shall support separate operator and administrator functions. The operator functions shall be restricted to those necessary for performing routine operations. The operator functions* shall allow the enabling and disabling of peripheral devices, mounting of removable storage media, backing-up and recovering user objects; maintaining the TCB hardware and software elements (e.g., on-site testing); and starting

and shutting down the system. ***The administrative functions shall support separate security administrator and auditor roles. The TCB shall enable the administrators to perform their functions only after taking distinct auditable action to assume an administrator role. Non-security functions that can be performed in the security administrative role shall be limited strictly to those essential to performing the security role effectively.[SM-4]***

5. The use of the protected mechanisms for system administration shall be limited to authorized administrative users.

Requirements for Reference Mediation

RM-3 Mediation of References to Subject and Object Attributes

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.

2. Reference mediation shall include control of references to all subjects, objects, and resources protected under the TCB security policy, to their policy (*i.e., access rights, security levels*) and status attributes (e.g., existence, length, locking state).

3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

Requirements for Logical TCB Protection

P-3 TCB Isolation and Timing Consistency

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Non-circumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

TCB protection shall also maintain the consistency of TCB global variables and eliminate undesirable dependencies of the TCB on unprivileged subject or user actions.

3. Consistency of TCB global variables requires that consistency conditions defined over TCB internal variables, objects, and functions hold before and after any TCB invocation.

4. Elimination of undesirable dependencies of the TCB on unprivileged subject actions requires that any TCB invocation by an unprivileged subject (or user) input to a TCB call may not place the TCB in a state such that it is unable to respond to communication initiated by other users.

Furthermore, TCB protection shall maintain the timing consistency of condition checks.

5. Timing consistency of condition checks requires that a validation check holds at the instant when the TCB action depending on that check is performed.

Requirements for TCB Self Checking

SC-1 Minimal Self Checking

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Requirements for TCB Start-Up and Recovery

TR-1 Minimal Requirements for Recovery or Start-up

Procedures and/or mechanisms shall be provided to assure that, after a TCB failure or other discontinuity, recovery without protection compromise is obtained.

Requirements for TCB Privileged Operation

PO-2 Privilege Association with TCB Modules

1. TCB privileges needed by individual functions, or groups of functions, of a functional component shall be identified. Privileged TCB calls or access to privileged TCB objects, such as user and group registration files, password files, security and integrity-level definition file, role definition file, audit-log file shall also be identified. It shall be possible to associate TCB privileges with TCB operations performed by administrative users.

2.The modules of a TCB function shall be associated only with the privileges necessary to complete their task.

3. Support for product privilege implementation and association with TCB modules provided by lower-level mechanisms or procedures (e.g., operating system, processors, language) shall be provided.

ASSURANCES

Requirements for TCB Property Definition

PD-3 Property Specification by Model Interpretation

The developer shall provide formal models for the functional components and sub-components of the profile. At a minimum, a formal model of the access control components shall be provided. The properties of the formal models shall be clearly stated. The developer shall provide an interpretation of the models in the DIS of the product's TCB. For each model entity, the developer shall: (1) identify the TCB elements and their DIS (if any) that implement that entity; (2) define the operation of these TCB elements, and (3) demonstrate, by coherent arguments, that the DIS of these elements is consistent with the model properties. The developer's interpretation of each formal model, which specifies the TCB properties, shall identify all TCB and DIS elements (if any) that do not correspond to any model entity and shall explain why these elements do not render the TCB properties invalid.

An informal model of reference mediation and TCB protection shall be provided. For the components that are not modeled, the developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement. The developer's interpretation of each functional requirement, which describes the TCB properties, shall include all the TCB elements.

Requirements for TCB Element Identification

ID-2: TCB Element Justification

The vendor shall identify the TCB elements (i.e., software, hardware/ firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).

The developer shall justify the protection relevance of the identified elements (i.e., only elements that can affect the correct operation of the protection functions shall be included in the TCB). If protection-irrelevant elements are included in the TCB, the developer shall provide a rationale for such inclusion.

Requirements for TCB Interface Definition

IF-2: Interface Descriptive Specification

The developer shall define all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB.

The developer shall provide and maintain a descriptive interface specification (DIS) of the TCB that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. The DIS shall identify the TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions signaled. The DIS shall also include the TCB call identifier, parameter types (e.g., input, output), the effect of the call, TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions handled and signaled. It shall be shown to be an accurate description of the TCB interface.

The DIS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.

If the TCB consists of a kernel and privileged processes, the developer shall separately identify and define the interfaces for the kernel and each privileged process.

The TCB interface definition must also include all effects of a call including the direct visibility and alterability of internal TCB variables and functions.

Requirements for TCB Modular Decomposition

MD-3: Module Relationship Analysis

The developer shall design the TCB as a small number (e.g., 10 to 100) of design and implementation subsystems that have well-defined functional relationships and shared-data dependencies. The developer shall identify the specific TCB protection properties and functions associated with each subsystem and the TCB interfaces (if any) implemented by each subsystem.

The developer shall design each subsystem as a set of modules. For each module, the developer shall describe: the role or purpose of the module, the set of related functions performed by the module, and the module interface (i.e., the set of invocable functions, calling conventions, parameters, global variables, and results). The developer shall identify the protection functions of, and describe the interfaces between, these modules. The developer shall choose the modules so that the set of functions implemented by the module, the module's contribution to the TCB protection properties, and the interface(s) to the module can be described concisely (e.g., the module shall have a single purpose). The TCB structuring into modules shall be based on well-defined module relationships; for example, the contains relation (e.g., A is part of B), the "uses" relation (e.g., A is correct only if B is correct). The developer shall analyze the correctness dependencies among these modules. This analysis may include, but is not restricted to, service and environmental dependencies.

Requirements for TCB Structuring Support

SP-3: Structured Protection Mechanisms

The TCB shall maintain process isolation. The TCB shall separate those elements that are protection-critical from those that are not. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate access-control attributes (e.g., readable, writable). The TCB shall employ a complete, conceptually simple, protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product.

Requirements for Design Disciplines

DD-2: Extended Disciplines for TCB Structuring

The developer shall design the product to minimize the complexity of the TCB. System engineering shall be directed towards excluding from the TCB modules that are not protection critical.

The TCB design shall reflect use of modern software engineering techniques), such as data hiding and abstraction (i.e., data, functional, and control abstractions) and well-defined exception-handling. The TCB design shall also include use of layering (including a rationale for each layering violation), high-level synchronization constructs, and multi-tasking/multi-threading.

Requirements for TCB Implementation Support

IM-3: Module Correspondence Support

The developer shall maintain engineering diagrams and source code (as applicable) for all TCB elements. The diagrams and source code for each module of the TCB shall be identified and provided as configuration items.

Requirements for Developer Functional Testing

FT-3: Specification-Driven TCB Interface Testing

The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description or specification. The tests shall exercise the boundary conditions of the protection functions. The developer shall generate the test conditions and data from the *Descriptive Interface Specification(s)*. The developer test procedures shall include the tests used to demonstrate the absence of all flaws discovered in previous versions of the TCB.

The developer shall correct all flaws discovered by testing and shall retest the TCB to show that all discovered flaws have been eliminated, no new flaws have been introduced, and the protection functions work as claimed.

Requirements for Penetration Analysis

PA-2 Flaw-Hypothesis Testing

The developer shall define the TCB configuration, interface, and protection functions that are subject to penetration testing. For each test, the developer shall identify the goal of the test and the criteria for successful penetration. The developer shall illustrate how, in addition to system reference manuals and TCB interface description, the DIS, source code, and hardware and firmware specifications are used to define penetration-test conditions. For each test, the developer shall document all test conditions, data (e.g., test set-up, function call parameters, and test outcomes), and coverage.

The developer shall generate the test conditions from flaw-hypotheses derived by negating assertions of TCB design capabilities and by providing counter examples that show that these assertions are false. The developer shall confirm the flaw hypotheses by checking design and implementation documentation, by defining the test data and running test programs, or by referring to known classes of penetration flaws found in other TCBs. The refutation of any hypothesis shall be documented.

For each uncovered flaw, the developer shall define and document scenarios of flaw exploitation and shall identify all penetration outcomes resulting from that scenario. The cause of the flaw shall be identified and documented.

Requirements for Covert-Channel Analysis

CCA-2 Timing Channel Analysis

1. *Identification:* The developer shall identify all sources of information used in covert-channel analysis. These sources shall include TCB reference manuals and DIS. The sources of information and methods of identification shall include processor specifications whenever the identification method includes source code and hardware analysis. The

developer shall define the identification method used. The developer shall demonstrate that the chosen identification method is sound (e.g., it leads to the discovery of all covert channels in the DIS or source documentation) and repeatable (i.e., independent evaluators can use the method on the same sources of covert-channel information and can obtain the same results.) The developer shall define scenarios of use for each covert channel. The developer shall also define timing channel scenarios, and shall identify all functions that provide independent sources of timing (e.g., CPUs, I/O processors).

2. *Bandwidth Measurement or Engineering Estimation:* The developer shall define the method used for covert-channel bandwidth estimation. In measuring TCB performance for covert-channel-bandwidth estimation, the developer shall satisfy the following assumptions. The maximum bandwidth estimation shall be based on the assumptions that the covert channel is noiseless, that the senders and receivers are not delayed by the presence of other processes in the product, and that the sender-receiver synchronization time is negligible. The choice of informal estimation methods shall define and justify the coding method and, therefore, the distribution of “0s” and “1s” in all transmissions.

The developer shall select TCB primitives to be measured for bandwidth determination from real scenarios of covert-channel use. The developer shall specify TCB measurement environment for the bandwidth measurements. This specification shall include: (1) the speed of the product functions, (2) the product configuration, (3) the sizes of the memory and cache components, and (4) the product initialization. The sensitivity of the measurement results to configuration changes shall be documented. The covert-channel measurements shall include the fastest TCB function calls for altering, viewing, and setting up the transmission environment; the demonstrably fastest process (context) switch time shall also be included in the bandwidth measurements. All measurements shall be repeatable.

3. *Covert Channel Testing:* The developer shall test all the use of all identified covert channels to determine whether the handling functions work as intended.

Requirements for User Guidance

UG-1: Users' Guide

The developer shall provide a User Guide which describes all protection services provided and enforced by the TCB. The User Guide shall describe the interaction between these services and provide examples of their use. The User Guide may be in the form of a summary, chapter or manual. The User Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

Requirements for Administrative Guidance

AG-3: Role-Based Administrative Guidance

The developer shall provide a Trusted Facility Manual intended for the product administrators and operators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB. The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy. The Trusted Facility Manual shall explain the unique security-relevant privileges and functions of administrators and operators. The Trusted Facility Manual shall also explain the distinct security-relevant privileges and functions of the TCB and how they can be selectively granted to provide fine-grained, multi-person or multi-role system and application administration policies. The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall identify all hardware, firmware, software, and data structures comprising the TCB. The detailed audit record structure for each type of audit event shall be described. *The Trusted Facility Manual shall explain how to configure the product to mitigate, eliminate, or audit covert channel exploitation*. The Trusted Facility Manual shall describe the cautions about and procedures for using the TCB as a base for site-specific secure applications. The Trusted Facility Manual shall describe procedures for securely regenerating the TCB after any part is changed (e.g., due to adding devices or installing flaw corrections to the TCB software).

The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.

Requirements for Trusted Generation

TG-3: Trusted Generation With Secure State Review

The developer shall establish and document the procedures that a consumer must perform to generate an operational TCB from the delivered copy of the master TCB. The consumer documentation shall identify any system parameters, which are initialized or set during system generation, that affect the TCB's conformance to the protection profile and state the acceptable ranges of values for those parameters. The product shall be delivered with each of these parameters set to its fail-safe defaults. The developer shall provide the consumer with a capability to review the product security state (e.g., by providing a program, which could be executed after generating and starting the TCB, that determines the consistency of the protection-relevant parameters).

Requirements for Life Cycle Definition

LC-3: Measurable Life Cycle Process

The developer shall develop and maintain the product using a well defined, standardized, and measurable engineering process. The developer shall explain why the process was chosen and how the developer uses it to develop and maintain the product. The developer shall comply with the engineering process standard. The process shall incorporate a security policy that states the technical, physical, procedural, personnel, and other measures used by the developer to protect the product and its documentation. The developer shall demonstrate that each development process and support process requirement of the protection profile is satisfied by some part, or parts, of the developer’s process. The developer shall identify the programming languages used to develop the TCB software and reference the definitions of those languages. The developer shall identify any implementation dependent options of the programming language compiler(s) used to implement the TCB software and reference the definitions of those languages.The developer shall describe coding standards followed during the implementation of the product and shall ensure that all source code complies with these standards.

Requirements for Configuration Management

CM-3: Comprehensive Automated Control

The developer shall establish configuration control and generation procedures employing automated tools for developing and maintaining the TCB. The procedures shall be employed to ensure that changes to the TCB are consistent with the product's protection properties and security policy. The developer shall employ these tools to track and control changes to development evidence, implementation data (e.g., source code and hardware diagrams), executable versions of the TCB, test documentation and procedures, identified flaws, and consumer documentation. The procedures shall include a formal acceptance process for protection-relevant changes.

The configuration control procedures shall assure a consistent mapping among documentation and code associated with the current version of the TCB and permit the regeneration of any supported version of the TCB. The developer shall provide tools for the generation of a new version of the TCB from source code. Also, tools shall be available for comparing a newly generated version with the previous TCB version to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

Requirements for Evidence of TCB Protection Properties

EPP-3 Evidence of Formal Model Interpretation in the DIS

The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. This documentation shall describe how the TCB implements the reference monitor concept. The developer shall also provide a formal access-control model and an informal reference mediation and TCB protection model. The TCB properties, which are defined by this correspondence and the interpretation of these models within the DIS of the TCB shall be documented by the product developer.

Requirements for Evidence of Product Development

EPD-4: Policy Consistency Of The DIS

The developer shall provide TCB Design Specifications that include: a list of the TCB elements (hardware, software, and firmware configuration items); a list of protection services provided to the TCB by hardware, software, and firmware that is not part of the TCB; an explanation of the techniques and criteria used during the modular decomposition of the TCB; a description of the policy allocations, functions, and interactions among the major TCB subsystems; and module level descriptions of all software and hardware in the TCB.

The developer shall provide a Descriptive Interface Specification (DIS) that describes the functions, effects, exceptions and error messages visible at the TCB interface and includes a convincing argument that the DIS is consistent with the formal model of the policy. The developer shall show that the DIS is an accurate representation of the TCB's external interfaces.

The developer shall provide TCB Implementation Data consisting of the engineering diagrams for all hardware included in the TCB and the source code used to generate the TCB software and firmware. The developer shall show that the TCB software, firmware, and hardware implement the documented TCB design.

Requirements for Evidence of Functional Testing

EFT-3: Evidence of Specification-Driven Testing

The developer shall provide evidence of the functional testing that includes the test plan, the test procedures, and the results of the functional testing. The test, plans, procedures, and results shall be maintained under the same configuration control as the TCB software. The test plans shall identify the TCB specification used in the derivation of the test conditions, data, and coverage analysis.

Requirements for Evidence of Penetration Analysis

EPA-2: Evidence of Flaw-Hypothesis Generation and Testing

The developer shall provide evidence of penetration testing. The penetration evidence shall identify all product documentation and development evidence on which the search for flaws was based. The penetration evidence shall describe the scenarios for exploiting each potential flaw in the system and the penetration test conditions, data (e.g., test set-up, function call parameters, and test outcomes), coverage, and conclusions derived from each scenario. The penetration evidence shall summarize both refuted and confirmed flaws hypothesis.

Requirements for Evidence of Covert Channel Analysis

ECC-2: Evidence of Covert Channel Analysis and Handling

The developer's documentation shall present the results of the covert channel analysis and the trade-offs involved in restricting these channels. All auditable events that may be used in the exploitation of known covert channels shall be identified. The developer shall provide the bandwidths of known covert channels whose use is not detectable by the auditing mechanism. The documentation of each identified covert channel shall consist of the variables, timing sources, and the TCB interface functions that can be used to transmit information. The measurements of each TCB function call used by covert channels must be documented and the bandwidth computation shall be included for each channel. The measurement environment should be documented as specified. Test documentation shall include results of testing the effectiveness of the methods used to reduce covert-channel bandwidths.

Requirements for Evidence of Product Support

EPS-3: Evidence of Measured Product Support

The developer shall provide documentation that defines, explains, and justifies the policies, procedures, plans, and tools established by the developer to satisfy the Operational Support and Development Environment requirements of the protection profile. The documentation shall also explain how the developer periodically evaluates compliance with the established procedures, policies, and plans.

Requirements for Test Analysis

TA-4: Comprehensive Test Analysis

The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and penetration analysis, and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results, and general correctness (e.g., defect trend from regression testing). This analysis shall examine the testability of requirements, the adequacy of the tests to measure the required properties, the deviation of the actual results obtained from the expected results. The analysis shall extend to trace all defects identified, corrected, and retested. The analysis shall include an assessment of test coverage and completeness, and defect frequency. The results of testing shall be interpreted in terms that express product performance and protection adequacy. The evaluator shall determine whether the product's protection properties, as defined for all protection-relevant modules of the TCB, and all relevant known penetration flaws have been tested. The evaluator shall independently develop, test, and document additional flaw hypotheses. The evaluator shall assess testing results to determine whether the product’s TCB works as claimed, that the TCB’s implementation is consistent with the DIS, and whether there are any obvious ways (i.e., ways that are known, or that are readily apparent or easily discovered in product documentation) for an unauthorized user to bypass the policy implemented by the TCB or otherwise defeat the product’s TCB, and whether all discovered TCB flaws have been corrected and no new TCB flaws introduced. No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. ***The testing results shall show that the methods used to reduce covert channel bandwidths have been effective for all evaluated configurations.*** The evaluator shall determine whether the product is relatively resistant to penetrations.

Requirements for Independent Testing

IT-3: Comprehensive Independent Testing.

The evaluator shall independently perform functional and elementary penetration testing to confirm test results. This testing may be selective and shall be based on (1) the results of other independent and/or producer testing, (2) the TCB’s DIS, (3) other product design and implementation documentation, (4) the product's user and administrative documentation, (5) relevant known penetration flaws**,** and (6) evaluator-developed TCB penetration flaw hypotheses and corresponding tests that attempt to exploit the hypothesized flaws. Satisfactory completion consists of demonstrating that all TCB functions work as described in the product's relevant documentation, that test results are consistent, and that no discrepancies exist between the documentation and the product. Satisfactory penetration test completion shall be determined by the subjective judgement (which may be supported algorithmically) of the evaluator. Test duration agreements may further constrain this judgement. Categorization of an actual penetration flaw shall be based on the reproducibility of that flaw. Flaws that are discovered, but are not reproducible shall remain categorized as potential penetration flaws. All actual penetration flaws must be corrected and retested.

The evaluator shall provide a penetration test plan document that describes the additional evaluator-developed flaw hypotheses and associated tests. The evaluator shall execute these tests and shall report any discovered flaws to the producer as part of the testing results. At the conclusion of penetration testing, the evaluator shall provide copies of this penetration test plan and its test results to the producer. The producer shall ensure that this test plan and its test results are incorporated into the rest of the product's testing documentation and that such documentation is available for further analysis throughout the life of the product.

The evaluator shall test for covert channel bandwidth reductions to determine the effectiveness of handling method(s) in reducing the bandwidths of identified covert channels for all evaluated configurations.

If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results. The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results. The evaluator shall also confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.

Requirements for Development Environment

DER-3: Comprehensive Development Environment Review

The evaluator shall review the producer's development and maintenance process description documentation and shall conduct a complete audit of the producer's processes using the evidence generated by each process to determine the degree of discipline enforced upon and within the process, and to determine the protection characteristics associated with the product's development and maintenance. The results of this review shall establish, for the evaluator, the producer's development environment, its policies, and the degree of enforcement maintained during development execution. The review shall also confirm the producer's complete conformance with all relevant development environment requirements.

Requirements for Operational Support

OSR-3 Comprehensive Operational Support Review

The evaluator shall review all documentation focused on the activities of product use (e.g., Users Manuals) and product administration including installation, operation, maintenance, and trusted recovery (e.g., Trusted Facility Management manuals. This review shall assess the clarity of presentation, difficulty in locating topics of interest, ease of understanding, and completeness of coverage. The need for separate manuals dedicated to protection-relevant aspects of the product should be assessed for effectiveness. The evaluator shall execute all documented protection-relevant features and procedures to determine if their descriptions are accurate and correct.

Requirements for Design Analysis

DA-3: Comprehensive Design Analysis

The evaluator shall determine whether the producer has performed the activities defined in the development process assurance requirements of the protection profile for TCB property definition and TCB design. The evaluator shall determine whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze, with the help of formal methods and appropriate automated tools, the results of the producer's activities for completeness, consistency, and correctness of design with respect to requirements (e.g., validating the formal verification of the design).

Requirements for Implementation

CI-3: Comprehensive Implementation Analysis

The evaluator shall conduct an inspection on a moderate sample of randomly selected product code. The assessment shall focus on the clarity of the coding style, adherence to coding standards, coding documentation, and on possible software defects that may be present with respect to the product’s formal design and model. The inspection shall be performed to obtain only a sample of possible software defects, not to capture all such possible defects. The evaluator shall report all discovered defects to the producer; the assessment shall report the number of defects found per line of code inspected from the random sample size. Use of producer-provided code inspection results can supplement this inspection. All trapdoors built into the product for maintenance purposes shall be identified by the producer and shown to be protected by the product. The producer shall correct all discovered defects and the corrected software reinspected. A rigorous analysis of the implementation's correspondence to the verified design shall be performed by the evaluator to validate correctness. Such analysis may be supported by appropriate automated tools.

DRAFT

LABEL BASED PROTECTION

FOR

MULTI-USER INFORMATION SYSTEMS

LEVEL 4

(LP-4)

A Protection Profile
Derived from the Federal Criteria for IT Security

Version 1.0

December 1992

This document is undergoing review and is subject to modification or withdrawal. The contents of this document should not be referenced in other publications.

Supersedes the
Trusted Computer System Evaluation Criteria
Class A1

DRAFT

LABEL-BASED PROTECTION - 4 (LP-4)

This Protection Profile has been developed to define a set of technical measures that can be incorporated into remote-access, resource- and information-sharing Information Technology (IT) products that will be used to protect two or more levels of National Security Information classified according to US Executive Order 12356 (EO 12356). This profile can also be used to protect any information that has been designated as sensitive information for which information separation and access are based on sensitivity markings applied to the information. This profile is intended for use in environments where the presence potentially malicious application software (e.g., Trojan Horses) mandate the use of high-assurance products.

Compliant IT products will provide highly-structured, conceptually simple protection mechanisms for a multi-level information processing environment with which an organization can construct an automated information system to enhance or optimize the organization's ability to perform its mission. Formal assurance of security policy support and covert channel analysis must be available. Compliant IT products are maintained under very strict configuration management facilities and can only be distributed via a trusted distribution channel.

LP-4 compliant products are functionally equivalent to those satisfying profile LP3 in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specifications and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal interface specification (FIS) of the design. Independent of the particular specification language or verification system used, there are five important criteria for profile LP-4 design verification:

a. A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model interpretation in the TCB is valid (i.e., the model interpretation is consistent with the model axioms) and is sufficient to support the security policy.

b. *A FIS must be produced that includes abstract definitions of the functions the TCB performs and of the hardware and/or firmware mechanisms that are used to support separate execution domains.*

c. *The FIS of the TCB must be shown to be consistent with the model by formal techniques where possible (i.e., where verification tools exist) and informal ones otherwise.*

d. *The TCB implementation (i.e., in hardware, firmware, and software) must be informally shown to be consistent with the FIS. The elements of the FIS must be shown, using informal techniques, to correspond to the elements of the TCB. The FIS must express the unified protection mechanism required to satisfy the security policy, and it is the elements of this protection mechanism that are mapped to the elements of the TCB.*

e. *Formal analysis techniques must be used to identify and analyze covert channels. Informal techniques may be used to identify covert timing channels. the continued existence of identified covert channels in the system must be justified.*

In keeping with the extensive design and development analysis of the TCB required of LP4 compliant systems, stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

Cross References:

- Existing Criteria:
  (1) TCSEC: A1

  (2) ITSEC

  (3) CTCPEC
- Other Protection Profiles
  (1) TBD

COMPONENT SUMMARY:

LP-4 Functional Component Summary

Functional Component	Code & Level
Security Policy Support	
Accountability	
Identification & Authentication	I&A-2
System Entry	----
Trusted Path	TP-2
Audit	AD-1+
Access Control	AC-3+
Discretionary	AC-3+
Non-Discretionary	AC-3
Covert Channel Handling	CCH-3
Availability	----
Resource Allocation	----
Fault Tolerance	----
Security Mgmt.	SM-1++
Reference Mediation	RM-3
TCB Logical Protection	P-3
TCB Physical Protection	----
TCB Self-checking	SC-1
TCB Start-Up and Recovery	TR-1
TCB Privileged Operation	PO-2
TCB Ease-of-Use	----

LP-4 Functional Component Summary

Assurance Component Summary	**T7**
Development Assurance Components	
Development Process	
TCB Property Definition	PD-4
TCB Design	
TCB Element Identification	ID-2
TCB Interface Definition	IF-3
TCB Modular Decomposition	MD-3
TCB Structuring Support	SP-3
TCB Design Disciplines	DD-2
TCB Implementation Support	IM-4

Assurance Component Summary	T7
TCB Testing & Analysis	
Functional Testing	FT-3
Penetration Analysis	PA-2
Covert Channel Analysis	CCA-3
Operational Support	
User's Security Guidance	UG-1
Administrative Guidance	AG-3
Trusted Generation	TG-3
Development Environment	
Life Cycle Definition	LC-3
Configuration Management	CM-4
Trusted Distribution	TD-1
Development Evidence	
TCB Protection Properties	EPP-4
Product Development	EPD-5
Product Testing & Analysis	
Functional Testing	EFT-3
Penetration Analysis	EPA-2
Covert Channel Analysis	ECC-2
Product Support	EPS-3
Evaluation Assurance Components	
Testing	
Test Analysis	TA-5
Independent Testing	IT-4
Review	
Development Environment	DER-3
Operational Support	OSR-3
Analysis	
Design	DA-3
Implementation	CI-3

RATIONALE

16. Information Protection Policy

It is anticipated that organizations wishing to process two to three levels of classified information with multiple categories will want to use IT products that are compliant with this profile in their automated information processing systems. These organizations should be able to trust the profile-compliant IT product to contribute to the protection of the classified information at least as much as they trust the properly cleared personnel who are using and managing the system.

17. Protection Philosophy

This profile presumes a hostile environment with divided, aggressive users. It provides control of access to shared resources both (1) on the basis of attributes that are controlled by the ordinary users of the system and (2) on the basis of attributes that are controlled only by the system administrators.

Profile compliant IT products will minimally meet the following objectives:

a. Employ a reference validation mechanism to enforce a formally defined security policy that describes the rules for controlling access to system subjects and objects and use the access control rules to enforce an information flow policy that aims to control the use of covert storage and timing channels.

b. Associate explicit sensitivity labels with each subject and object in the system and each port through which information may be exported from or imported to the system. Maintain the accuracy of the sensitivity labels as information moves within the system and through the ports.

c. Authenticate the claimed identity of each external human user of the IT product prior to establishing any internal entity to act on behalf of that user and firmly bind the authenticated user identity to the internal entity.

d. Selectively keep and protect a log of all actions or events (including use of covert storage channels) that could affect system security so that they can be accurately attributed to the known user or system entity responsible for causing the action or event. Also, alert the system administrator when a series of events indicates an imminent violation of the security policy.

e. Contains hardware and software mechanisms that can be independently evaluated to provide sufficient assurance that the system satisfies the previous four objectives.

f. Implements the enforcement of objectives a through d in such a fashion that the enforcing mechanisms are protected from tampering and unauthorized changes by the information moving entities that the mechanisms are supposed to control.

18. Expected Threats

The requirements for profile conforming IT products assume that these products are being used in an environment where there are different levels and categories of classified data and users of differing clearance levels. A conforming IT product can be reasonably expected to protect the confidentiality of information in an environment where there are three levels and multiple categories of classified data, and two or more levels of cleared users and where there are collaborating, malicious users and software at each clearance level.

19. Assumed Environment

19.1 Characteristics

IT products complying with the requirements set forth in this profile are expected to be used in an environment with the following characteristics:

a. Multiple users will be accessing the operating system at the same time.

b. The IT product hardware base (e.g., CPU, printers, terminals, etc.) is protected from unauthorized physical access.

c. One or more personnel are assigned to manage the system in which the IT product is incorporated, including the security of the information it contains.

d. A need to control user access to information exists and is based on an explicit sensitivity marking associated with the information (e.g, Secret or Top Secret).

e. There is a need to control user access to information exists and is based on that user's identity and membership in organizations or groups.

f. The IT product provides facilities for some or all of the authorized users to create programs that use the applications programming interface (API) and make those programs available to other users.
g. The IT product is used to provide a cooperative environment for the users to accomplish some task or group of tasks.

19.2 Environment Dependencies

Secure installation and operation of a product satisfying these profile requirements depends on provision of a number of elements in the installation environment. These include:

a. Physical security must be provided. For US Government classified operation, physical security equivalent to PP-2 would be required.
b. Cabling to other devices must be shown to be consistent with policy implemented by the product. For example, a “port” in the product is required to have an assigned label. No device can be connected to the port unless it has been established externally that the device is allowed to receive data with the same label.
c. Personnel allowed to access data processed by the installed product must already be authorized for such access.

20. Intended Use

Conforming IT products are useful in both general-purpose office automation environments with multiple data sensitivities (or “classifications”) and multiple levels of user authorizations (or “clearances”) and in specialized computing, network and mission environments. Examples of the office automation environment might include military headquarters and highly competitive procurement offices. Examples of the network environments include use as the basis for a multilevel secure network management center or a trusted guard gateway operating between two networks processing different levels of information. An example of the specialized mission environment might be as a platform for a portable battlefield map and mission management application.

FUNCTIONAL REQUIREMENTS

Requirements for Identification and Authentication

I&A-2 Identification, Authentication, and Authorization

1. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2. The TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the *clearance and authorization of individual users.* These data shall be used by the TCB to authenticate the user's identity and to ensure *that the subject security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user).*

3. The TCB shall protect authentication data so that it cannot be used by any unauthorized user.

Requirements for Trusted Path

TP-2 Trusted User-to-TCB Communication

The TCB shall support a trusted communication path between itself and users for use whenever a positive user-to-TCB connection is required (e.g., login, change of policy attributes). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other communication paths.

Requirements for Audit

AD-1+ Minimal Audit

1. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.

2. The TCB shall be able to record the following types of events:

- use of the identification and authentication mechanisms;

- introduction of objects into a user’s address space (e.g., file open, program initiation), and deletion of objects;

- actions taken by computer operators and system administrators and/or system security officers.

The TCB shall be able to record any override of human-readable output markings. The TCB shall also be able to audit the identified event that may be used in the exploitation of covert channels.

The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of auditable events that may indicate an imminent violation of the product's security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded, and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event. [AD-3]

3. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user’s address space and for object deletion events the audit record shall include the name and the *object security level.*

4. The system administrator shall be able to selectively audit the actions of one or more users based on individual identity and/or *object security level.*

Requirements for Access Control

AC-3 + Extended Access Control

1. Definition of Access Control Attributes

The TCB shall define and protect access control attributes for subjects and objects. Subject attributes shall include named individuals or defined groups or both. Object attributes shall include defined access rights (e.g., read, write, execute) that can be assigned to subject attributes. *Access control attributes corresponding to each individual policy shall be identified.*

Sensitivity labels associated with each subject and storage object that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. The sensitivity labels shall be used as the basis for mandatory access control decisions.

The subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels.

The subject and object attributes shall accurately reflect the sensitivity and integrity of the subject or object. *When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.*

The TCB shall immediately notify a terminal user of each *change in the security level associated with that user during an interactive session.* A terminal user shall be able to query the TCB as desired for a display of the subject's complete *sensitivity label.*

The TCB shall support the assignment of *minimum and maximum security levels* to all attached physical devices. These *security levels* shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

2. Administration of Access Control Attributes

The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects. The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users. These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. *(i.e., these rules shall define the distribution, revocation, and review of access control attributes). The controls defined by these rules shall be capable of specifying for each named object, a list of individuals and a list of groups of named individuals, with their respective access rights to that object. Furthermore, for each named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is given [AC-4}.* These controls shall be capable of including or excluding access to the granularity of a single user.

The rules for assignment and modification of access control attributes shall include those for attribute assignment to objects during import and export operations.

Export of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

1. Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

2. Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3. Labeling Human-Readable Output

The system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

Import of Non-labeled Data

In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

3. Authorization of Subject References to Objects

The TCB shall define and enforce authorization rules for the mediation of subject references to objects. These rules shall be based on the access control attributes of subjects and objects. These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

The scope of the authorization rules shall include all subjects, storage objects (e.g., processes, segments, devices) and associated access control attributes that are directly or indirectly accessible to subjects external to the TCB. The scope of the authorization rules shall *also include all policy and status attributes of subjects and storage objects (e.g., quotas, object existence, size, access time, creation and modification time, locked/ unlocked).* If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.

The authorization rules for the mandatory access control policy shall include:

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices that are directly or indirectly accessible by subjects external to the TCB. The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non- hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

The authorization rules for each policy shall be defined separately. The TCB shall define and enforce the composition of policies, including the enforcement of the authorization rules (e.g., subject and object type coverage, enforcement precedence).

4. Subject and Object Creation and Destruction

The TCB shall control the creation and destruction of subjects and objects. These controls shall include object reuse. That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects; information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.

Requirements for Covert Channel Handling

CCH-3 Timing Channel Audit and Bandwidth Limitation

1. The TCB and privileged applications shall include functions that help audit the use of covert storage channels. These functions shall enable the identification of the transmitter, receiver, and specific covert channels used (e.g., TCB and privileged application element used to transmit information). TCB functions that help limit the bandwidth and/or eliminate covert storage channels shall also be provided. The bandwidth limits for each channel shall be settable by system administrators.

2. The functions added to the TCB and privileged applications for storage channel auditing shall be identified for each channel and shall be available in common product configurations. If audit functions are not added to certain storage channels (e.g., hardware storage channels), evidence must be provided to justify why these channels do not represent a security threat for the intended use of the product. TCB and privileged application functions that help limit the bandwidth and/or eliminate covert storage or timing channels shall also be available in common product configurations.

If channel bandwidth limitation and channel elimination functions are not added to certain storage or timing channels (e.g., hardware channels), evidence must be provided to justify why these channels do not represent a security threat for the intended use of the product.

Requirements for Security Management

SM-1++ Minimal Security Management

1. The TCB shall provide an installation mechanism for the setting and updating of its configuration parameters, and for the initialization of its protection-relevant data structures before any user or administrator policy attributes are defined. It shall allow the configuration of TCB internal databases and tables.

2. The TCB shall provide protected mechanisms for displaying and modifying the security policy parameters.

3. The TCB shall provide protected mechanisms for manually displaying, modifying, or deleting user registration and account parameters. These parameters shall include unique user identifiers, their account, and their associated user name and affiliation. The TCB shall allow the manual enabling and disabling of user identities and/or accounts.

4. *The TCB shall support separate operator and administrator functions. The operator functions shall be restricted to those necessary for performing routine operations. The operator functions* shall allow the enabling and disabling of peripheral devices, mounting of removable storage media, backing-up and recovering user objects; maintaining the TCB hardware and software elements (e.g., on-site testing); and starting

and shutting down the system. *The administrative functions shall support separate security administrator and auditor roles. The TCB shall enable the administrators to perform their functions only after taking distinct auditable action to assume an administrator role. Non-security functions that can be performed in the security administrative role shall be limited strictly to those essential to performing the security role effectively.[SM-4]*

5. The use of the protected mechanisms for system administration shall be limited to authorized administrative users.

Requirements for Reference Mediation

RM-3 Mediation of References to Subject and Object Attributes

1. The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications. The mediation shall ensure that all references are directed to the appropriate security-policy functions.

2. Reference mediation shall include control of references to all subjects, objects, and resources protected under the TCB security policy, to their policy (*i.e., access rights, security levels*) and status attributes (e.g., existence, length, locking state).

3. References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

Requirements for Logical TCB Protection

P-3 TCB Isolation and Timing Consistency

The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:

1. TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code, (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.

2. Non-circumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.

TCB protection shall also maintain the consistency of TCB global variables and eliminate undesirable dependencies of the TCB on unprivileged subject or user actions.

3. Consistency of TCB global variables requires that consistency conditions defined over TCB internal variables, objects, and functions hold before and after any TCB invocation.

4. Elimination of undesirable dependencies of the TCB on unprivileged subject actions requires that any TCB invocation by an unprivileged subject (or user) input to a TCB call may not place the TCB in a state such that it is unable to respond to communication initiated by other users.

Furthermore, TCB protection shall maintain the timing consistency of condition checks.

5. Timing consistency of condition checks requires that a validation check holds at the instant when the TCB action depending on that check is performed.

Requirements for TCB Self Checking

SC-1 Minimal Self Checking

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Requirements for TCB Start-Up and Recovery

TR-1 Minimal Requirements for Recovery or Start-up

Procedures and/or mechanisms shall be provided to assure that, after a TCB failure or other discontinuity, recovery without protection compromise is obtained.

Requirements for TCB Privileged Operation

PO-2 Privilege Association with TCB Modules

1. TCB privileges needed by individual functions, or groups of functions, of a functional component shall be identified. Privileged TCB calls or access to privileged TCB objects, such as user and group registration files, password files, security and integrity-level definition file, role definition file, audit-log file shall also be identified. It shall be possible to associate TCB privileges with TCB operations performed by administrative users.

2.The modules of a TCB function shall be associated only with the privileges necessary to complete their task.

3. Support for product privilege implementation and association with TCB modules provided by lower-level mechanisms or procedures (e.g., operating system, processors, language) shall be provided.

ASSURANCES

Requirements for TCB Property Definition

PD-4 Formal Specification of TCB Properties

The developer shall provide formal models for the functional components and sub-components of the profile. At a minimum, a formal model of the access control components shall be provided. The properties of the formal models shall be clearly stated. The developer shall provide a formal interpretation of the models in the FIS of the product's TCB. For each model entity, the developer shall: (1) identify the TCB elements and their FIS (if any) that implement that entity; (2) specify the operation of these TCB elements, and (3) prove that the FIS of these elements is consistent with the model properties. The developer's interpretation of each formal model, which specifies the TCB properties, shall identify all TCB and FIS elements (if any) that do not correspond to any model entity and shall explain why these elements do not render the TCB properties invalid.

An informal model of reference mediation and TCB protection shall be provided. For the components that are not modeled, the developer shall interpret the functional requirements of the protection profile within the product TCB. For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement; (2) describe the operation of these TCB elements, and (3) explain why the operation of these elements is consistent with the functional requirement. The developer's interpretation of each functional requirement, which describes the TCB properties, shall include all the TCB elements.

Requirements for TCB Element Identification

ID-2: TCB Element Justification

The vendor shall identify the TCB elements (i.e., software, hardware/firmware code and data structures). Each element must be unambiguously identified by its name, type, release, and version number (if any).

The developer shall justify the protection relevance of the identified elements (i.e., only elements that can affect the correct operation of the protection functions shall be included in the TCB). If protection-irrelevant elements are included in the TCB, the developer shall provide a rationale for such inclusion.

Requirements for TCB Interface Definition

IF-3: Formal Interface Specification

The developer shall define all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB.

The developer shall provide and maintain a descriptive interface specification (DIS) of the TCB that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. The DIS shall identify the TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions signaled. The DIS shall also include the TCB call identifier, parameter types (e.g., input, output), the effect of the call, TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions handled and signaled. It shall be shown to be an accurate description of the TCB interface.

A Formal Interface Specification (FIS) of the TCB shall be maintained that accurately describes the TCB in terms of the call identifier, parameter types (e.g., input, output), the effect of the call, TCB call conventions (e.g., parameter order, call sequence requirements), and exceptions signaled.

The DIS and FIS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.

If the TCB consists of a kernel and privileged processes, the developer shall separately identify and define the interfaces for the kernel and each privileged process.

The TCB interface definition must also include all effects of a call including the direct visibility and alterability of internal TCB variables and functions.

Requirements for TCB Modular Decomposition

MD-3: Module Relationship Analysis

The developer shall design the TCB as a small number (e.g., 10 to 100) of design and implementation subsystems that have well-defined functional relationships and shared-data dependencies. The developer shall identify the specific TCB protection properties and functions associated with each subsystem and the TCB interfaces (if any) implemented by each subsystem.

The developer shall design each subsystem as a set of modules. For each module, the developer shall describe: the role or purpose of the module, the set of related functions performed by the module, and the module interface (i.e., the set of invocable functions, calling conventions, parameters, global variables, and results). The developer shall identify the protection functions of, and describe the interfaces between, these modules. The developer shall choose the modules so that the set of functions implemented by the module, the module's contribution to the TCB protection properties, and the interface(s) to the module can be described concisely (e.g., the module shall have a single purpose). The TCB structuring into modules shall be based on well-defined module relationships; for example, the contains relation (e.g., A is part of B), the “uses” relation (e.g., A is correct only if B is correct). The developer shall analyze the correctness dependencies among these modules. This analysis may include, but is not restricted to, service and environmental dependencies.

Requirements for TCB Structuring Support

SP-3: Structured Protection Mechanisms

The TCB shall maintain process isolation. The TCB shall separate those elements that are protection-critical from those that are not. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate access-control attributes (e.g., readable, writable). The TCB shall employ a complete, conceptually simple, protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product.

Requirements for Design Disciplines

DD-2: Extended Disciplines for TCB Structuring

The developer shall design the product to minimize the complexity of the TCB. System engineering shall be directed towards excluding from the TCB modules that are not protection critical.

The TCB design shall reflect use of modern software engineering techniques), such as data hiding and abstraction (i.e., data, functional, and control abstractions) and well-defined exception-handling. The TCB design shall also include use of layering (including a rationale for each layering violation), high-level synchronization constructs, and multi-tasking/multi-threading.

Requirements for TCB Implementation Support

IM-4: Naming Support For Design Correspondence

The developer shall maintain engineering diagrams and source code (as applicable) for all TCB elements. The developer shall identify the programming languages used to develop the TCB software and reference the definitions of those languages. The developer shall identify any implementation dependent options of the programming language compiler(s) used in the TCB source code. The developer shall describe coding standards followed during the implementation of the product and shall ensure that all source code complies with these standards. The diagrams and source code for each module of the TCB shall be identified and provided as configuration items. The diagrams and source code shall be named using the same conventions as those used in the TCB design. The developer shall explain how the programming languages used help establish the correspondence between the TCB implementation and design.

Requirements for Developer Functional Testing

FT-3: Specification-Driven TCB Interface Testing

The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description or specification. The tests shall exercise the boundary conditions of the protection functions. The developer shall generate the test conditions and data from the *Descriptive Interface Specification(s)*. The developer test procedures shall include the tests used to demonstrate the absence of all flaws discovered in previous versions of the TCB.

The developer shall correct all flaws discovered by testing and shall retest the TCB to show that all discovered flaws have been eliminated, no new flaws have been introduced, and the protection functions work as claimed.

Requirements for Penetration Analysis

PA-2 Flaw-Hypothesis Testing

The developer shall define the TCB configuration, interface, and protection functions that are subject to penetration testing. For each test, the developer shall identify the goal of the test and the criteria for successful penetration. The developer shall illustrate how, in addition to system reference manuals and TCB interface description, the DIS, source code, and hardware and firmware specifications are used to define penetration-test conditions. For each test, the developer shall document all test conditions, data (e.g., test set-up, function call parameters, and test outcomes), and coverage.

The developer shall generate the test conditions from flaw-hypotheses derived by negating assertions of TCB design capabilities and by providing counter examples that show that these assertions are false. The developer shall confirm the flaw hypotheses by checking design and implementation documentation, by defining the test data and running test programs, or by referring to known classes of penetration flaws found in other TCBs. The refutation of any hypothesis shall be documented.

For each uncovered flaw, the developer shall define and document scenarios of flaw exploitation and shall identify all penetration outcomes resulting from that scenario. The cause of the flaw shall be identified and documented.

Requirements for Covert-Channel Analysis

CCA-3 Formal Covert Channel Analysis

1. *Identification:* The developer shall identify all sources of information used in covert-channel analysis. These sources shall include TCB reference manuals, DIS, and FIS. The sources of information and methods of identification shall include processor specifications whenever the identification method includes source code and hardware analysis. The developer shall define the identification method used. The developer shall define the identification method used. The developer shall demonstrate that the chosen identification method is sound (e.g., it leads to the discovery of all covert channels in the FIS or source documentation) and repeatable (i.e., independent evaluators can use the method on the same sources of covert-channel information and can obtain the same results.) The method shall be applied on the FIS of the TCB, and shall include syntactic information-flow analysis (with or without the use of semantic analysis) or noninterference analysis. The identification of covert channels shall include specification-to-code correspondence.

The developer shall define scenarios of use for each cover channel. The developer shall also define timing channel scenarios, and shall identify all functions that provide independent sources of timing (e.g., CPUs, I/O processors).

2. *Bandwidth Measurement or Engineering Estimation:* The developer shall define the method used for covert-channel bandwidth estimation. The method shall be based on information theory methods. In measuring TCB performance for covert-channel-bandwidth estimation, the developer shall satisfy the following assumptions. The maximum bandwidth estimation shall be based on the assumptions that the covert channel is noiseless, that the senders and receivers are not delayed by the presence of other processes in the product, and that the sender-receiver synchronization time is negligible.

The developer shall select TCB primitives to be measured for bandwidth determination from real scenarios of covert channel use. The developer shall specify TCB measurement environment for the bandwidth measurements. This specification shall include: (1) the speed of the product functions, (2) the product configuration, (3) the sizes of the memory and cache components, and (4) the product initialization. The sensitivity of the measurement results to configuration changes shall be documented. The covert-channel measurements shall include the fastest TCB function calls for altering, viewing, and setting up the transmission environment; the demonstrably fastest process (context) switch time shall also be included in the bandwidth measurements. All measurements shall be repeatable.

3. *Covert Channel Testing:* The developer shall test all the use of all identified covert channels to determine whether the handling functions work as intended.

Requirements for User Guidance

UG-1: Users' Guide

The developer shall provide a User Guide which describes all protection services provided and enforced by the TCB. The User Guide shall describe the interaction between these services and provide examples of their use. The User Guide may be in the form of a summary, chapter or manual. The User Guide shall specifically describe user responsibilities. These shall encompass any user responsibilities identified in the protection profile.

Requirements for Administrative Guidance

AG-3: Role-Based Administrative Guidance

The developer shall provide a Trusted Facility Manual intended for the product administrators and operators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy. The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB. The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy. The Trusted Facility Manual shall explain the unique security-relevant privileges and functions of administrators and operators. The Trusted Facility Manual shall also explain the distinct security-relevant privileges and functions of the TCB and how they can be selectively granted to provide fine-grained, multi-person or multi-role system and application administration policies. The Trusted Facility Manual shall describe the administrative interaction between security services.

The Trusted Facility Manual shall identify all hardware, firmware, software, and data structures comprising the TCB. The detailed audit record structure for each type of audit event shall be described. *The Trusted Facility Manual shall explain how configure the product to mitigate, eliminate, or audit their exploitation.* The Trusted Facility Manual shall describe the cautions about and procedures for using the TCB as a base for site-specific secure applications. The Trusted Facility Manual shall describe procedures for securely regenerating the TCB after any part is changed (e.g., due to adding devices or installing flaw corrections to the TCB software).

The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.

Requirements for Trusted Generation

TG-3: Trusted Generation With Secure State Review

The developer shall establish and document the procedures that a consumer must perform to generate an operational TCB from the delivered copy of the master TCB. The consumer documentation shall identify any system parameters, which are initialized or set during system generation, that affect the TCB's conformance to the protection profile and state the acceptable ranges of values for those parameters. The product shall be delivered with each of these parameters set to its fail-safe defaults. The developer shall provide the consumer with a capability to review the product security state (e.g., by providing a program, which could be executed after generating and starting the TCB, that determines the consistency of the protection-relevant parameters).

Requirements for Life Cycle Definition

LC-3: Measurable Life Cycle Process

The developer shall develop and maintain the product using a well defined, standardized, and measurable engineering process. The developer shall explain why the process was chosen and how the developer uses it to develop and maintain the product. The developer shall comply with the engineering process standard. The process shall incorporate a security policy that states the technical, physical, procedural, personnel, and other measures used by the developer to protect the product and its documentation. The developer shall demonstrate that each development process and support process requirement of the protection profile is satisfied by some part, or parts, of the developer's process. The developer shall identify the programming languages used to develop the TCB software and reference the definitions of those languages. The developer shall identify any implementation dependent options of the programming language compiler(s) used to implement the TCB software and reference the definitions of those languages.The developer shall describe coding standards followed during the implementation of the product and shall ensure that all source code complies with these standards.

Requirements for Configuration Management

CM-4: Extended Configuration Management

The developer shall establish configuration control and generation procedures employing automated tools for developing and maintaining the TCB. The procedures shall be employed to ensure that all changes to the TCB are consistent with the product's protection properties and security policy. The developer shall employ these tools to track and control changes to development evidence, implementation data (e.g., source code and hardware diagrams), executable versions of the TCB, test documentation and procedures, identified flaws, and consumer documentation. The procedures shall include a formal acceptance process for protection-relevant changes.

The configuration control procedures shall assure a consistent mapping among documentation and code associated with the current version of the TCB and permit the regeneration of any supported version of the TCB. The developer shall provide tools for the generation of a new version of the TCB from source code. Also, tools shall be available for comparing a newly generated version with the previous TCB version to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB. The developer shall use a combination of technical, physical, and procedural safeguards to protect the master copy or copies of all material used to generate the TCB from unauthorized modification or destruction.

Requirements for Trusted Distribution

TD-1: TCB Modification Detection During Distribution

The developer shall establish procedures and employ appropriate technical measures to detect modifications to any TCB-related software, firmware, and hardware, including updates, that is transferred from the development environment to a consumer’s site.

Requirements for Evidence of TCB Protection Properties

EPP-4 Evidence of Formal Model Interpretation in the FIS

The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces. This documentation shall describe how the TCB implements the reference monitor concept. The developer shall also provide a formal access-control model and an informal reference mediation and TCB protection model. The TCB properties, which are defined by this correspondence and the interpretation of these models within the DIS and FIS of the TCB shall be documented by the product developer.

Requirements for Evidence of Product Development

EPD-5: Policy Consistency Of The FIS

The developer shall provide a Descriptive Interface Specification (DIS) that describes the functions, effects, exceptions and error messages visible at the TCB interface and includes a convincing argument that the DIS is consistent with the formal model of the policy. The developer shall show that the DIS is an accurate representation of the TCB's external interfaces.

The developer shall provide a Formal Interface Specification (FIS) that rigorously defines the protection functions available at the TCB interface in terms of: the protection properties implemented by each function, the precise semantics for invoking each function, the effects of each function (i.e., returned values and effect on the TCB state), and the possible exceptions and error messages returned by each function. The FIS shall be accompanied by a convincing argument that it is consistent with the formal model of the product protection policy. This argument shall be constructed using both manual and machine-assisted specification and verification methods. Machine-assisted specification and verification methods shall be approved by the product evaluation authority.

The developer shall provide TCB Design Specifications that include: a list of the TCB elements (hardware, software, and firmware configuration items); a list of protection services provided to the TCB by hardware, software, and firmware that is not part of the TCB; an explanation of the techniques and criteria used during the modular decomposition of the TCB; a description of the policy allocations, functions, and interactions among the major TCB subsystems; module level descriptions of all software and hardware in the TCB; and an argument that the design implements exactly the functions specified in the FIS.

The developer shall provide TCB Implementation Data consisting of the engineering diagrams for all hardware included in the TCB and the source code used to generate the TCB software and firmware. The developer shall show, through either manual or machine-assisted correspondence methods, that the TCB software, firmware, and hardware implement the documented TCB design.

Requirements for Evidence of Functional Testing

EFT-3: Evidence of Specification-Driven Testing

The developer shall provide evidence of the functional testing that includes the test plan, the test procedures, and the results of the functional testing. The test, plans, procedures, and results shall be maintained under the same configuration control as the TCB software. The test plans shall identify the TCB specification used in the derivation of the test conditions, data, and coverage analysis.

Requirements for Evidence of Penetration Analysis

EPA-2: Evidence of Flaw-Hypothesis Generation and Testing

The developer shall provide evidence of penetration testing. The penetration evidence shall identify all product documentation and development evidence on which the search for flaws was based. The penetration evidence shall describe the scenarios for exploiting each potential flaw in the system and the penetration test conditions, data (e.g., test set-up, function call parameters, and test outcomes), coverage, and conclusions derived from each scenario. The penetration evidence shall summarize both refuted and confirmed flaws hypothesis.

Requirements for Evidence of Covert Channel Analysis

ECC-2: Evidence of Covert Channel Analysis and Handling

The developer's documentation shall present the results of the covert channel analysis and the trade-offs involved in restricting these channels. All auditable events that may be used in the exploitation of known covert channels shall be identified. The developer shall provide the bandwidths of known covert channels whose use is not detectable by the auditing mechanism. The documentation of each identified covert channel shall consist of the variables, timing sources, and the TCB interface functions that can be used to transmit information. The measurements of each TCB function call used by covert channels must be documented and the bandwidth computation shall be included for each channel. The measurement environment should be documented as specified. Test documentation shall include results of testing the effectiveness of the methods used to reduce covert-channel bandwidths.

Requirements for Evidence of Product Support

EPS-3: Evidence of Measured Product Support

The developer shall provide documentation that defines, explains, and justifies the policies, procedures, plans, and tools established by the developer to satisfy the Operational Support and Development Environment requirements of the protection profile. The documentation shall also explain how the developer periodically evaluates compliance with the established procedures, policies, and plans.

Requirements for Test Analysis

TA-5: Formal Test Analysis

The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and penetration analysis, and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results, and general correctness (e.g., defect trend from regression testing). This analysis shall examine the testability of requirements, use of the FIS for test derivation, the adequacy of the tests to measure the required properties, the deviation of the actual results obtained from the expected results. The analysis shall extend to trace all defects identified, corrected, and retested. The analysis shall include an assessment of test coverage and completeness, and defect frequency. The results of testing shall be interpreted in terms that express product performance and protection adequacy. The evaluator shall determine whether the product's protection properties, as defined for the entire TCB, and all relevant known penetration flaws have been tested. The evaluator shall independently develop, test, and document additional flaw hypotheses. The evaluator shall assess testing results to determine whether the product’s TCB works as claimed, that the TCB’s implementation is consistent with the FIS, and whether there are any obvious ways (i.e., ways that are known, or that are readily apparent or easily discovered in product documentation) for an unauthorized user to bypass the policy implemented by the TCB or otherwise defeat the product’s TCB, and whether all discovered TCB flaws have been corrected and no new TCB flaws introduced. No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. If covert channel handling methods have been implemented, the testing results shall show that the methods used to reduce covert channel bandwidths have been effective for all evaluated configurations. The evaluator shall determine whether the product is completely resistant to penetrations.

IT-4: Formal Independent Testing.

The evaluator shall independently perform functional and elementary penetration testing to confirm test results. This testing shall be based on (1) the results of producer or other independent testing, (2) the TCB’s FIS, (3) the product’s design and implementation documentation, (4) the product's user and administrative documentation, (5) relevant known penetration flaws, and (6) evaluator-developed TCB penetration flaw hypotheses and corresponding tests that attempt to exploit the hypothesized flaws. Satisfactory completion consists of demonstrating that all TCB functions work as described in the product's relevant documentation, that the TCB functions are consistent with the FIS, that test results are consistent, and that no discrepancies exist between the documentation and the product.

Satisfactory penetration test completion shall be determined by the subjective judgement of the evaluator (which may be supported algorithmically). Test duration agreements may further constrain this judgement. Categorization of an actual penetration flaw shall be based on the reproducibility of that flaw. Flaws that are discovered, but are not reproducible shall remain categorized as potential penetration flaws. All actual penetration flaws must be corrected and retested.

The evaluator shall provide a penetration test plan document that describes the additional evaluator-developed flaw hypotheses and associated tests. The evaluator shall execute these tests and shall report any discovered flaws to the producer as part of the testing results. At the conclusion of penetration testing, the evaluator shall provide copies of this penetration test plan and its test results to the producer. The producer shall ensure that this test plan and its test results are incorporated into the rest of the product's testing documentation and that such documentation is available for further analysis throughout the life of the product.

The evaluator shall test for covert channel bandwidth reductions to determine the effectiveness of handling method(s) in reducing the bandwidths of identified covert channels.

Requirements for Development Environment

DER-3: Comprehensive Development Environment Review

The evaluator shall review the producer's development and maintenance process description documentation and shall conduct a complete audit of the producer's processes using the evidence generated by each process to determine the degree of discipline enforced upon and within the process, and to determine the protection characteristics associated with the product's development and maintenance. The results of this review shall establish, for the evaluator, the producer's development environment, its policies, and the degree of enforcement maintained during development execution. The review shall also confirm the producer's complete conformance with all relevant development environment requirements.

Requirements for Operational Support

OSR-3 Comprehensive Operational Support Review

The evaluator shall review all documentation focused on the activities of product use (e.g., Users Manuals) and product administration including installation, operation, maintenance, and trusted recovery (e.g., Trusted Facility Management manuals. This review shall assess the clarity of presentation, difficulty in locating topics of interest, ease of understanding, and completeness of coverage. The need for separate manuals dedicated to protection-relevant aspects of the product should be assessed for effectiveness. The evaluator shall execute all documented protection-relevant features and procedures to determine if their descriptions are accurate and correct.

Requirements for Design Analysis

DA-3: Comprehensive Design Analysis

The evaluator shall determine whether the producer has performed the activities defined in the development process assurance requirements of the protection profile for TCB property definition and TCB design. The evaluator shall determine whether the producer has documented these activities as defined in the development evidence requirements of the protection profile. The evaluator shall analyze, with the help of formal methods and appropriate automated tools, the results of the producer's activities for completeness, consistency, and correctness of design with respect to requirements (e.g., validating the formal verification of the design).

Requirements for Implementation

CI-3: Comprehensive Implementation Analysis

The evaluator shall conduct an inspection on a moderate sample of randomly selected product code. The assessment shall focus on the clarity of the coding style, adherence to coding standards, coding documentation, and on possible software defects that may be present with respect to the product’s formal design and model. The inspection shall be performed to obtain only a sample of possible software defects, not to capture all such possible defects. The evaluator shall report all discovered defects to the producer; the assessment shall report the number of defects found per line of code inspected from the random sample size. Use of producer-provided code inspection results can supplement this inspection. All trapdoors built into the product for maintenance purposes shall be identified by the producer and shown to be protected by the product. The producer shall correct all discovered defects and the corrected software reinspected. A rigorous analysis of the implementation’s correspondence to the verified design shall be performed by the evaluator to validate correctness. Such analysis may be supported by appropriate automated tools.