# Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness

**Version 1.22**

## Information Assurance Directorate

**National Security Agency**
**9800 Savage Road**
**Fort George G. Meade, MD 20755-6000**

**23 May 2001**

# Foreword

1 This publication, "*Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness*", is issued by the Information Assurance Directorate as part of its program to promulgate security standards for information systems. This protection profile is based on the "Common Criteria for Information Technology Security Evaluations, Version 2.1."

2 Further information, including the status and updates, of this protection profile can be found on the internet at: http://www.iatf.net/protection_profiles/index.cfm.

3 Comments on this document should be directed to: ppcomments@iatf.net. The comments should include the title of the document, the page, the section number, and paragraph number, detailed comment and recommendations.

# Table of Contents

# List of Figures

# List of Tables

# 1. Introduction

4 This section contains overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The PP identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The PP overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The overview can also be used as a stand-alone abstract for PP catalogues and registers. The "Conventions" section provides the notation, formatting, and conventions used in this protection profile. The "Glossary of Terms" section gives a basic definition of terms, which are specific to this PP. The "Document Organization" section briefly explains how this document is organized.

## 1.1 Identification

5 Title: Protection Profile For Multilevel Operating Systems In Environments Requiring Medium Robustness Version 1.22, 23 May 2001

6 Registration: Information Assurance Directorate

7 Keywords: operating system, COTS, medium robustness, multilevel, access control, mandatory access control, MAC, discretionary access control, DAC, labels, integrity, cryptography, mandatory integrity control, MIC, cryptography

## 1.2 Overview

8 The "*Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness"* specifies security requirements for commercial-off-the-shelf (COTS) general-purpose multilevel operating systems in networked environments containing sensitive information[1]. This profile makes use of Department of Defense (DoD) Information Assurance (IA) guidance and policy as a basis to establish the requirements necessary to achieve the security objectives of the Target of Evaluation (TOE) and its environment.

9 Operating systems evaluated against this PP will associate sensitivity labels with all objects and all its users will have an associated clearance level identifying the maximum security level of data that they may access. Operating systems evaluated against this PP can operate in the following multilevel environments:

- processing data up to the Secret level with uncleared authorized users,
- processing data up to the Top Secret level with minimum user clearances of Secret, and
- processing data up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level with minimum user clearances of Top Secret.

[1] See "Glossary of Terms" section for definition of "sensitive information".

10 Conformant products support Identification and Authentication, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Mandatory Integrity Control (MIC), an audit capability, and cryptographic services. These systems provide adequate security services, mechanisms, and assurances to process up to classified information in medium robustness environments, as specified in the "Guidance and Policy for Department of Defense Information Assurance[2]" (GiG). They can process mission supportive and mission administrative information. Mission critical information may be processed only if the environment provides the mechanisms to ensure availability of the data residing in the TOE (e.g., mirrored/duplicated data).

11 PP conformant systems may be suitable for use in non-DoD environments. The mechanisms specified by this PP may be appropriate for the protection of administrative, private, and sensitive information. When a company's most sensitive information is to be sent over a publicly accessed network, the company should apply additional protection at the network boundaries.

## 1.3 Mutual Recognition of Common Criteria Certificates

12 The assurance requirements contained in this PP meet the Evaluated Assurance Level (EAL) four augmented (4+), as defined in the "Common Criteria for Information Technology Security Evaluation Version 2.1" (CC). COTS operating systems meeting the requirements of this profile support the United States DoD multilevel medium robustness environments as described in GiG policy. However, under the "Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security" document, only CC requirements certificates at or below EAL 4 are mutually recognized. Because this profile exceeds the limits imposed by the "Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security" document, the US DoD will recognize only certificates issued by the US evaluation scheme to meet this profile. Other national schemes are under no obligation to recognize US certificates with assurance components exceeding EAL4.

## 1.4 Conventions

13 The notation, formatting, and conventions used in this protection profile (PP) are consistent with version 2.1 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

14 The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 2, paragraph 2.1.4 as:

assignment: allows the specification of an identified parameter;

refinement: allows the addition of details or the narrowing of requirements;

[2] Attachment 2: "GIG IA Implementation Guidance", Section 5.1.2 of the "DoD Chief Information Officer, Guidance and Policy Memorandum No. 6-8510" dated 16 June 2000.

selection: allows the specification of one or more elements from a list; and

iteration: allows a component to be used more than once with varying operations.

15 *Assignments or selections* left to be specified by the developer in subsequent security target documentation are italicized and identified between brackets ("[ ]"). In addition, when an assignment or selection has been left to the discretion of the developer, the text "assignment:" or "selection:" is indicated within the brackets. Assignments or selection created by the PP author (for the developer to complete) are bold, italicized, and between brackets ("[ ]"). CC selections completed by the PP author are underlined and CC assignments completed by the PP author are bold.

16 *Refinements* are identified with "**Refinement:**" right after the short name. They permit the addition of extra detail when the component is used. The underlying notion of a refinement is that of narrowing. There are two types of narrowing possible: narrowing of implementation and narrowing of scope[3]. Additions to the CC text are specified in bold. Deletions of the CC text are identified in the "End Notes" with a bold number after the component ("**8**").

17 *Iterations* are identified with a number inside parentheses ("(#)"). These follow the short family name and allow components to be used more than once with varying operations.
*Explicit Requirements* are allowed to create requirements should the Common Criteria not offer suitable requirements to meet the PP needs. The naming convention for explicit requirements is the same as that used in the CC. To ensure these requirements are explicitly identified, the ending "**_EXP**" is appended to the newly created short name. This PP uses US CC interpretations, which are also incorporated as explicitly specified components. These component short names end with "_US_INTERP_EXP". All element short names are inherited from the component name, but to clearly identify which element is the US CC interpretation, only the short names of these elements are bolded. The rationale for creating a requirement is provided in Section 7.5.

18 *Application Notes* are used to provide the reader with additional requirement understanding or to clarify the author's intent. These are italicized and usually appear following the element needing clarification.

19 These conventions are expressed by using combinations of bolded, italicized, and underlined text as specified in Table 1.1.

**Table 1.1 - Functional Requirements Operation Conventions**

[3] US interpretation #0362: Scope of Permitted Refinements at http://www.radium.ncsc.mil/tpep/library/interps/0362.html

| Convention | Purpose | Operation |
|---|---|---|
| **Bold** | The purpose of bolded text is used to alert the reader that additional text has been added to the CC. This could be an assignment that was completed by the PP author or a refinement to the CC statement.<br>Examples:<br>FMT_MSA.3.2 The TSF shall allow the **authorized administrator** to specify alternative initial values to override the default values when an object or information is created.<br>FPT_ITT.3.1 **Refinement:** The TSF shall be able to detect <u>modification and substitution of data</u> for TSF data transmitted between separate parts of the TOE **through the use of cryptographic means**. | (Completed) Assignment<br>or<br>Refinement |
| *Italics* | The purpose of italicized text is to inform the reader of an assignment or selection operation to be completed by the developer or ST author. It has been left as it appears in the CC requirement statement.<br>Examples:<br>FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].<br>FPT_ITT.2.1 The TSF shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between separate parts of the TOE. | Assignment (to be completed by developer or ST author)<br>or<br>Selection (to be completed by developer or ST author) |
| <u>Underline</u> | The purpose of underlined text is to inform the reader that a choice was made from a list provided by the CC selection operation statement.<br>Example:<br>FAU_STG.1.2 The TSF shall be able to <u>prevent</u> modifications to the audit records. | Selection (completed by PP author) |

| Convention | Purpose | Operation |
|---|---|---|
| ***Bold & Italics*** | The purpose of bolded and italicized text is to inform the reader that the author has added new text to the requirement and that an additional vendor action needs to be taken.<br>Example:<br>FIA_UAU.1.1 **Refinement:** The TSF shall allow **read access to *[assignment: list of public objects]*** on behalf of the user to be performed before the user is authenticated.<br>FCS_CKM.2.1 – The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***[selection: Manual (Physical) Method, Automated (Electronic Method), Manual Method and Automated Method]*** that meets the … | Assignment<br>(added by the PP author for the developer or ST author to complete)<br>or<br>Selection<br>(added by the PP author for the developer or ST author to complete) |
| Parentheses<br>(Iteration #) | The purpose of using parentheses and an iteration number is to inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times. Iterations are performed at the component level. The component behavior name includes information specific to the iteration between parentheses.<br>Example:<br>5.5.3.1 Management of TSF Data (for general TSF data) (FMT_MTD.1(1))<br>FMT_MTD.1.1(1) The TSF shall restrict the ability to **create**, query, modify, delete, and clear the **security-relevant TSF data except for audit records, user security attributes, authentication data, and critical security parameters** to **the authorized administrator**.<br>5.5.3.2 Management of TSF Data (for audit records) (FMT_MTD.1(2))<br>FMT_MTD.1.1(2) The TSF shall restrict the ability to change default, query, delete, and clear the **audit records** to **authorized administrators**. | Iteration 1<br>(of component)<br>Iteration 2<br>(of component) |

| Convention | Purpose | Operation |
|---|---|---|
| Explicit: (**_EXP**) | The purpose of using **Explicit:** before the family or component behavior name is to alert the reader and to explicitly identify a newly created component. To ensure these requirements are explicitly identified, the "**_EXP**" is appended to the newly created short name and the family or component name is bolded. This PP uses US CC interpretations, which are also incorporated as explicitly specified components. These short names end with "**_US_INTERP_EXP**". All element short names are inherited from the component name, but to clearly identify which element is the US CC interpretation, only the short names of these elements are bolded.<br><br>Example:<br>**5.2.1.2 Explicit: Cryptographic Key Handling and Storage (FCS_CKM_EXP.2)**<br><br>**FCS_CKM_EXP.2.1:** The TSF shall perform key entry and output in accordance with FIPS PUB 140-1**.**<br><br>**5.3.2.1 Explicit: Security Attribute Based Access Control (FDP_ACF_US_INTERP_EXP.1)**<br><br>**FDP_ACF_US_INTERP_EXP.1.1** The TSF shall enforce the **Discretionary Access Control policy** to objects based on the following types of subject and object security attributes.<br><br>FDP_ACF_US_INTERP_EXP.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among subjects and **named** objects is allowed … | Explicit Requirement<br><br>or<br><br>US Interpretation as an explicit component |

| Convention | Purpose | Operation |
|---|---|---|
| Endnotes | The purpose of endnotes is to alert the reader that the author has deleted Common Criteria text. An endnote number is inserted at the end of the requirement, and the endnote is recorded on the last page of the section. The endnote statement first states that a deletion was performed and then provides the rationale. Following is the family behavior or requirement in its original and modified form. A strikethrough is used to identify deleted text and bold for added text. A text deletion rationale is provided. Examples:<br><br>Text as shown:<br><br>FPT_TST.1.2 **Refinement:** The TSF shall provide authorized **administrators** with the capability to verify the integrity of TSF data.**18**<br><br>Endnote statement:<br><br>**18** A deletion of CC text was performed in FPT_TST.1.2. Rationale: The word " users " was deleted to replace it with the role of "authorized administrator". Only authorized administrators should be given the capability to verify the integrity of the TSF data.<br><br>FPT_TST.1.2 **Refinement:** The TSF shall provide authorized ~~users~~ **administrators** with the capability to verify the integrity of TSF data. | Refinement |

# 1.5 Glossary of Terms

20 This profile uses the terms described in this section to aid in the application of the requirements. The numbers specified between brackets ("[#]") at the end of some definitions point to the “References” section to identify where these definitions were obtained.

| | |
|---|---|
| Access | A specific type of interaction between a subject and an object that results in the flow of information from one to the other [10]. |
| Asymmetric Cryptographic System | A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key). |
| Asymmetric key | The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system. |

| | |
|---|---|
| Authorized administrator | An authorized user who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given to them. |
| Authorized user | A user who has been uniquely identified and authenticated. These users are considered to be legitimate users of the TOE. |
| Clearance | The users maximum authorization composed of a combination of sensitivity level and integrity level. |
| Component | The smallest selectable set of elements that may be included in a PP, an ST, or a package. |
| Critical Security Parameters (CSP) | Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module. |
| Cryptographic administrator | An authorized user who has been granted the authority to perform cryptographic initialization and management functions. These users are expected to use this authority only in the manner prescribed by the guidance given to them. |
| Cryptographic boundary | An explicitly defined contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module. |
| Cryptographic key (key) | A parameter used in conjunction with a cryptographic algorithm that determines [7]:<br>– the transformation of plaintext data into ciphertext data,<br>– the transformation of ciphertext data into plaintext data,<br>– a digital signature computed from data,<br>– the verification of a digital signature computed from data, or<br>– a data authentication code computed from data. |
| Cryptographic Module | The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. |
| Cryptographic Module Security Policy | A precise specification of the security rules under which a cryptographic module must operate, including the rules derived from the requirements of this PP and additional rules imposed by the vendor. |

| | |
|---|---|
| Discretionary Access Control (DAC) | 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 [10]. |
| Element | Individual requirements within a CC component; cannot be selected individually for inclusion in a PP, ST, or package. |
| Embedded Cryptographic Module | One that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system). |
| Evaluation Assurance Level (EAL) | A package consisting of assurance components from CC, part 3 that represents a point on the CC predefined assurance scale. |
| Enclave | An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security and therefore protected from other environments. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN) or be based on physical location and proximity [2]. |
| Integrity label | A security attribute that represents the integrity level of a subject or an object. Integrity labels are used by the TOE as the basis for mandatory integrity control decisions. |
| Integrity level | The combination of a hierarchical level and an optional set of non-hierarchical categories that represent the integrity of the information [10]. |
| Level of Robustness | The characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly to support the level of concern assigned to a particular information system. DoD has three levels of robustness [2]:<br>a. High: security services and mechanisms that provide the most stringent available protection and rigorous security countermeasures<br>b. Medium: security services and mechanisms that provide for layering of additional safeguards above the DoD minimum (Basic).<br>c. Basic: security services and mechanisms that equate to good commercial practices. |

| | |
|---|---|
| Mission Category | Reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD has three mission categories [2]:<br>a. Mission critical. Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.<br>b. Mission support. Systems handling information that is important to the support of deployed and contingency forces; must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness.<br>c. Administrative. Systems handling information which is necessary for the conduct of day-to- day business, but does not materially affect support to deployed or contingency forces in the short term. |
| Mandatory Access Control (MAC) | A means of restricting access to objects based on subject and object sensitivity labels.[4] |
| Mandatory Integrity Control (MIC) | A means of restricting access to objects based on subject and object integrity labels.[5]. |
| Multilevel system | A system that can simultaneously handle (e.g., share, process) multiple levels of data. It allows users at different sensitivity levels to access the system concurrently. The system permits each user to access only the data to which they are authorized access. |

[4] The Bell LaPadula model is an example of Mandatory Access Control

[5] The Biba integrity model is an example of Mandatory Integrity Control.

| | |
|---|---|
| Named Object | An object that exhibits all of the following characteristics:<br>- The object may be used to transfer information between subjects of differing user identities within the TSF.<br>- Subjects in the TOE must be able to request a specific instance of the object.<br>- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.<br>- The intended use of the object is for sharing of information across user identities. [11] |
| Object | An entity within the TOE security functions scope of control (TSC) that contains or receives information and upon which subjects perform operations. |
| Operating Environment | The total environment in which an information system operates. It includes the physical facility and controls, procedural and administrative controls, and personnel controls [2]. |
| Operational key | Key intended for protection of operational information or for the production or secure electrical transmissions of key streams. |
| Public Object | An object for which the TSF unconditionally permits all subjects "read" access. Only the TSF or privileged subjects may create, delete, or modify the public objects. No discretionary access checks or auditing are required for "read" accesses to such public objects. Attempts to create, delete, or modify such objects shall be considered security-relevant events, and, therefore, controlled and auditable. Objects that all subjects can read (e.g., the system clock) must be, implicitly, system low. [11] |
| Protection Profile (PP) | An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs. |
| Security attributes | TSF data that contains information about subjects and objects and upon which access control decisions are based. |
| Security level | The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity on the information [10]. |
| Security Target (ST) | A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE. |

| | |
|---|---|
| Sensitive information | Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. [10] |
| Sensitivity label | A security attribute that represents the security level of an object and that describes the sensitivity (e.g. Classification) of the data in the object. Sensitivity labels are used by the TOE as the basis for mandatory access control decisions [10]. |
| Split key | A variable that consists of two or more components that must be combined to form the operational key variable. The combining process excludes concatenation or interleaving of component variables. |
| Subject | An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects may be exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies. |
| Symmetric key | A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms. |
| Target of Evaluation (TOE) | An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation [1]. |
| TOE Security Functions (TSF) | A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP [1]. |
| Unauthorized user | A user who may obtain access only to system provided public objects if any exist. |
| User | A term used to include both authorized and unauthorized users. |

## 1.6 Document Organization

21 *Section 1* provides the introductory material for the protection profile.

22 *Section 2* describes the Target of Evaluation in terms of its envisaged usage and connectivity.

23 *Section 3* defines its expected security environment in terms of the threats to its security, the security assumptions made about its use, and the security policies that must be followed.

24 *Section 4* identifies the security objectives derived from these threats and policies.

25 *Section 5* identifies and defines the security functional requirements from the Common Criteria that must be met by the TOE in order for the functionality-based objectives to be met.

26 *Section 6* identifies the security assurance requirements.

27 *Section 7* provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

28 *Section 8* identifies background material used as reference to create this profile.

29 *Appendix A* defines frequently used acronyms.

30 *Appendix B* lists cryptographic standards, policies, and other related publications that have been identified in section 5 of this protection profile.

# 2. Target of Evaluation (TOE) Description

## 2.1 Product Type

31 This protection profile specifies DoD requirements for general-purpose multi-user COTS multilevel operating systems together with the underlying hardware that supports these systems. Such operating systems are typically employed in a networked office automation environment (see Figure 2.1) containing file systems, printing services, network services and data archival services and can host other applications (e.g., mail, databases). This profile does not specify any security characteristics of security hardened devices (e.g. guards, firewalls) that provide environment protection at network boundaries. **When this TOE is used in composition with other systems to make up a larger system environment, the boundary protection must provide the appropriate security mechanisms, cryptographic strengths and assurances to ensure adequate protection for the security and integrity of this TOE.**

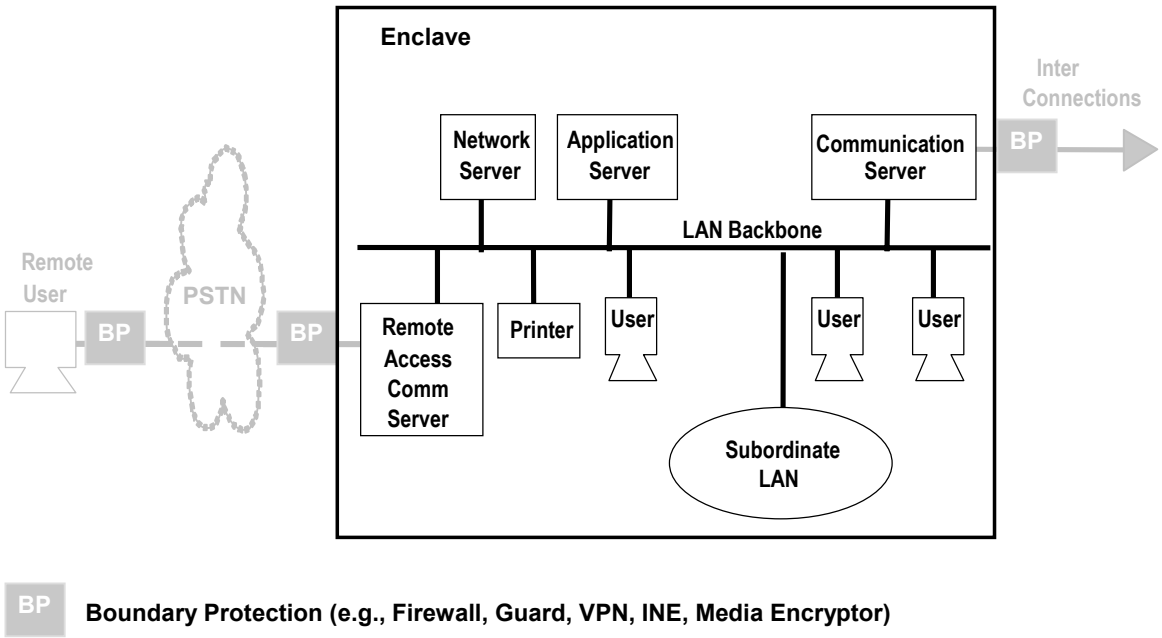


**Figure 2.1 TOE Environment**

## 2.2 General TOE Functionality

32 Conformant operating systems include the following security features:

- Identification and Authentication which mandates authorized users to be uniquely identified and authenticated before accessing information stored on the system;

- Discretionary Access Control (DAC) which restricts access to objects based on the identity of subjects and/or groups to which they belong, and allows authorized users to specify protection for objects that they control;
- Mandatory Access Control (MAC) which enforces the U.S. DoD data sensitivity classification model (i.e., Unclassified, Secret, Top Secret) on all authorized users and all TOE resources;
- Mandatory Integrity Control (MIC) which enforces an integrity policy on all authorized users and TOE resources to prevent malicious entities from corrupting data;
- Cryptographic services which provide mechanisms to protect TSF code and data and also provide support to allow authorized users and applications to encrypt and digitally sign data as it resides within the system and as it is transmitted to other systems; and
- Audit services which allow authorized administrators to detect and analyze potential security violations.

33 Other characteristics of complaint TOEs include:

- the ability to process multiple security levels of information in a multilevel environment,
- the inability to provide mechanisms or services to ensure availability of data residing on the TOE. [If availability requirements exist, the environment must provide the required mechanisms (e.g., mirrored/duplicated data)], and
- the inability to provide complete physical protection mechanisms, which must likewise be provided by the environment.

## 2.3 Cryptographic Requirements

34 The TOE cryptographic services must provide both a level of functionality and assurance regardless of its implementation (software, hardware, or any combination thereof). This is achieved by meeting both the NIST FIPS PUB140-1 standard and all additional requirements as stated in this PP (refer to Appendix B for relevant cryptographic standards, policies, and other publications).

35 For cryptographic services fully implemented in hardware, all FIPS 140-1 Level 3 requirements as well as all additional requirements identified in this PP, must be met. For all other implementations (i.e., software or a combination of software/hardware), the requirements identified in FIPS 140-1 Level 1[6] and all-additional requirements identified in this PP must be met. These two implementations, with the exception of the Electromagnetic Interference/Electromagnetic Compatibility requirements, are equivalent in intent and counter the identified threats in this PP. For convenience, section 5.2 of this protection profile identifies

[6] The overall NIST rating for software and/or a combination of software and hardware must meet FIPS PUB 140-1 Level 1. However, this PP requires the cryptographic module to meet higher NIST ratings in certain security areas. These additional requirements are identified within this PP.

where a NIST certification is required and against what standard. The evaluation laboratory will use both the NIST certification and their evaluation results on the additional requirements to determine if the vendor has met section 5.2.

## 2.4 TOE Operational Environment

36 This profile makes use of the Defense-in-Depth[7] (D-i-D) strategy to allow the use of COTS products in DoD environments containing sensitive information. The fundamental principle of robustness of IA technology solutions is used to provide an effective set of safeguards tailored according to each organization's unique needs. The D-i-D strategy establishes policy necessary to counter threats and achieve security objectives. The characterization of the strength of the security functions, mechanisms, services or solutions, and the assurance (or confidence) that these are implemented and functioning correctly determine the level of robustness of the TOE.

37 The intended robustness level of the TOE environment is medium robustness[8]. This level of robustness and the systems' evaluated assurance levels allows the TOE environment to process:

- data up to the Secret level with uncleared authorized users,
- data up to the Top Secret level with minimum user clearances of Secret, and
- data up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level with minimum user clearances of Top Secret.

38 The information processed by these systems can be mission supportive and/or mission administrative. If availability requirements exist (processing of mission critical information), the environment must provide the required mechanisms (e.g., mirrored/duplicated data).

39 The target environments in this profile are multilevel. The information processed can contain data of multiple security levels. All authorized users will have an associated clearance level identifying the maximum security level of data that may be accessed.

40 It is assumed that the TOE environment is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. This environment can be specific to an organization or a mission and may also contain multiple networks or enclaves. They may be logical, such as an operational area network (OAN) or be based on physical location and proximity.

41 The TOE may be accessible by external IT systems that are beyond the environment's security policies. The users of these external IT systems are similarly beyond the control of the operating

[7] Attachment 2: "GIG IA Implementation Guidance", Sections 1 and 3 of the "DoD Chief Information Officer, Guidance and Policy Memorandum No. 6-8510" dated 16 June 2000

[8] Minimum requirements for medium robustness are specified in the Attachment 2: "GIG IA Implementation Guidance", Section 5.1.2 of the "DoD Chief Information Officer, Guidance and Policy Memorandum No. 6-8510" dated 16 June 2000.

system's policies. Although the users of these external systems are authorized in their environments, they are outside the scope of control of this particular environment so nothing can be presumed about their intent. They must be viewed as hostile.

42 For non-DoD environments, mechanisms specified by this PP may be appropriate for protection of administrative, private, and sensitive information. When a company's most sensitive information is to be sent over a publicly accessible network; the company should consider applying additional layered security mechanisms.

# 3. TOE Security Environment

43 The security environment for the functions addressed by this specification includes threats, security policy, and usage assumptions, as discussed below.

## 3.1 Threats

44 Specific threats to IT security that should be countered by the operating system:

| | |
|---|---|
| T.ADMIN_ERROR | Improper administration may result in defeat of specific security features. |
| T.ADMIN_ROGUE | Authorized administrator's intentions may become malicious resulting in TSF data to be compromised. |
| T.AUDIT_CORRUPT | A malicious process or user may cause audit records to be lost or modified, or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions. |
| T.CONFIG_CORRUPT | A malicious process or user may cause configuration data or other trusted data to be lost or modified. |
| T.DATA_NOT_SEPARATED | Systems may not adequately separate data on the basis of its sensitivity or integrity label, thereby allowing users improper access to labeled data. |
| T.DOS | A malicious process or user may block others from system resources via a resource exhaustion denial of service attack. |
| T.EAVESDROP | A malicious process or user may intercept transmitted data inside or outside of the enclave. |
| T.IMPROPER_INSTALLATION | Operating system may be delivered, installed, or configured in a manner that undermines security. |
| T.INSECURE_START | Reboot may result in insecure state of the operating system. |
| T.MASQUERADE | A malicious process or user on one machine on the network may masquerade as an entity on another machine on the same network. |
| T.OBJECTS_NOT_CLEAN | Systems may not adequately remove the data from objects between usage by different users, thereby releasing information to a user unauthorized for the data. |
| T.POOR_DESIGN | Unintentional or intentional errors in requirement specification, design or development of the IT operating system may occur. |

| | |
|---|---|
| T.POOR_IMPLEMENTATION | Unintentional or intentional errors in implementing the design of the IT operating system may occur. |
| T.POOR_TEST | Incorrect system behavior may result from inability to demonstrate that all functions and interactions within the operating system operation are correct. |
| T.REPLAY | A malicious process or user may gain access by replaying authentication (or other) information. |
| T.SPOOFING | A hostile entity may masquerade itself as the IT operating system and communicate with authorized users who incorrectly believe they are communicating with the IT operating system. |
| T.SYSACC | A malicious process or user may gain unauthorized access to the administrator account, or that of other trusted personnel. |
| T.UNATTENDED_SESSION | A malicious process or user may gain unauthorized access to an unattended session. |
| T.UNAUTH_ACCESS | Unauthorized access to data by a user may occur. |
| T.UNAUTH_MODIFICATION | Unauthorized modification or use of IT operating system attributes and resources may occur. |
| T.UNDETECTED_ACTIONS | Failure of the IT operating system to detect and record unauthorized actions may occur. |
| T.UNIDENTIFIED_ACTIONS | Failure of the administrator to identify and act upon unauthorized actions may occur. |
| T.UNKNOWN_STATE | Upon failure of the IT operating system, the security of the IT operating system may be unknown. |
| T.USER_CORRUPT | User data may be lost or tampered with by other users. |

## 3.2 Security Policy

45 Policy statements whose enforcement must be provided by the operating system's security mechanisms:

| | |
|---|---|
| P.ACCESS_BANNER | The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. |
| P.ACCOUNT | The users of the system shall be held accountable for their actions within the system. |
| P.AUTHORIZATION | The system must limit the extent of each user's abilities in accordance with the TSP. |

| | |
|---|---|
| P.AUTHORIZED_USERS | Only those users who have been authorized to access the information within the system may access the system. |
| P.CLEARANCE | The system must limit access to protected resources to authorized users whose security and integrity levels are appropriate for the labeled data. |
| P.CRYPTOGRAPHY | The system shall use NIST FIPS validated cryptography (methods and implementations) for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services). |
| P.I_AND_A | All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects. |
| P.INDEPENDENT_TESTING | The operating system must undergo independent testing as part of an independent vulnerability analysis. |
| P.LABELED_OUTPUT | The beginning and end of all paged, hardcopy output must be marked with sensitivity labels that properly represent the sensitivity of the output. |
| P.NEED_TO_KNOW | The system must limit the access to the information in protected resources to those authorized users who have a need to know that information. |
| P.REMOTE_ADMIN_ACCESS | Authorized administrators may remotely manage the IT operating system. |
| P.RESOURCE_LABELS | All resources must have associated labels identifying the security and integrity levels of data contained therein. |
| P.ROLES | The authorized administrator and cryptographic administrator shall have separate and distinct roles associated with them. |
| P.SYSTEM_INTEGRITY | The system must have the ability to periodically validate its correct operation and, with the help of administrators, it must be able to recover from any errors that are detected. |
| P.TRACE | The operating system must have the ability to review the actions of individuals. |
| P.TRUSTED_RECOVERY | Procedures and/or mechanisms shall be provided to assure that, after a system failure or other discontinuity, recovery without a protection compromise is obtained |

| | |
|---|---|
| P.USER_CLEARANCE | All users must have a clearance level identifying the maximum security and integrity levels of data they may accessed. |
| P.VULNERABILITY_SEARCH | The system must undergo an analysis for vulnerabilities beyond those that are obvious. |

## 3.3 Security Usage Assumptions

46 Assumptions about the use of the IT operating system:

| | |
|---|---|
| A.PHYSICAL | It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information. |

# 4. Security Objectives

47 This section defines the security objectives for the TOE and its environment. These objectives are suitable to counter all identified threats and cover all identified organizational security policies and assumptions. The TOE security objectives are identified with "O." appended to at the beginning of the name and the environment objectives are identified with "OE." appended to the beginning of the name.

## 4.1 TOE Security Objectives

| | |
|---|---|
| O.ACCESS | The IT operating system will ensure that users gain only authorized access to it and to its resources that it controls. |
| O.ACCESS_HISTORY | The system will display information (to authorized users) related to previous attempts to establish a session. |
| O.ADMIN_ROLE | The operating system will provide an administrator role to isolate administrative actions. |
| O.ADMIN_TRAINED | The IT operating system will provide authorized administrators with the necessary information for secure management. |
| O.AUDIT_GENERATION | The IT operating system will provide the capability to detect and create records of security relevant events associated with users. |
| O. AUDIT_PROTECTION | The IT operating system will provide the capability to protect audit information. |
| O. AUDIT_REVIEW | The IT operating system will provide the capability to selectively view audit information. |
| O.CONFIG_MGMT | All changes to the operating system and its development evidence will be tracked and controlled. |
| O.DISCRETIONARY_ACCESS | The IT operating system will control accesses to resources based upon the identity of users and groups of users. |
| O.DISCRETIONARY_USER_CONTROL | The IT operating system will allow authorized users to specify which resources may be accessed by which users and groups of users. |
| O.DISPLAY_BANNERS | The system will display an advisory warning regarding use of the TOE. |

| | |
|---|---|
| O.ENCRYPTED_CHANNEL | Encryption will be used to provide confidentiality of TSF protected data in transit to remote parts of the TOE. |
| O.ENCRYPTION_SERVICES | The IT operating system will make encryption services available to authorized users and/or user applications. |
| O.INSTALL | The IT operating system will be delivered with the appropriate installation guidance to establish and maintain IT security. |
| O.MANAGE | The IT operating system will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the IT system. |
| O.MANDATORY_ACCESS | The IT operating system will control accesses to resources based upon the security levels of users and resources. |
| O.MANDATORY_INTEGRITY | The IT operating system will control accesses to resources based upon the integrity levels of users and resources. |
| O.MARKINGS | The IT operating system will provide the capability to mark printed output with accurate sensitivity labels. |
| O.PENETRATION_TEST | The operating system will undergo independent penetration testing to show that the system design and implementation are not bypassable. |
| O.PROTECT | The IT operating system will provide means to protect user data and resources. |
| O.RECOVERY | Procedures and/or mechanisms will be provided to assure that recovery is obtained without a protection compromise, such as from system failure or discontinuity. |
| O.RESIDUAL_INFORMATION | The IT operating system will ensure that any information contained in a protected resource is not released when the resource is reallocated. |
| O.RESOURCE_SHARING | No user will block others from accessing resources. |
| O.SELF_PROTECTION | The operating system will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure. |

| | |
|---|---|
| O.SOUND_DESIGN | The design of the IT operating system will be the result of sound design principles and techniques, which are accurately documented. |
| O.SOUND_IMPLEMENTATION | The implementation of the IT operating system will be an accurate instantiation of its design. |
| O.TESTING | The operating system will undergo independent testing, based at least in part upon an independent vulnerability analysis and includes test scenarios and results. |
| O.TRAINED_USERS | The IT operating system will provide authorized users with the necessary guidance for secure operation. |
| O.TRUSTED_PATH | The operating system will provide a means to ensure users are not communicating with some other entity pretending to be the operating system. |
| O.TRUSTED_SYSTEM_OPERATION | The IT operating system will function in a manner that maintains IT security. |
| O.TSF_CRYPTOGRAPHIC_INTEGRITY | The IT operating system will provide cryptographic integrity mechanisms for TSF data while in transit to remote parts of the TOE. |
| O.USER_AUTHENTICATION | The operating system will verify the claimed identity of the user. |
| O.USER_IDENTIFICATION | The operating system will uniquely identify users. |
| O.VULNERABILITY_ANALYSIS | The system will undergo an analysis for vulnerabilities beyond those that are obvious. |

## 4.2 Environment Security Objectives

| | |
|---|---|
| OE.PHYSICAL | Physical security will be provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information. |

# 5. Security Functional Requirements

48 This section contains detailed security functional requirements for the operating systems' trusted security functions (TSF) supporting multilevel systems in medium robustness environments. The requirements are applied against the operating system in conjunction with the underlying hardware that supports it. The requirements contained in this section are either selected from Part 2 of the CC or have been explicitly stated (with short names ending in "_EXP"). Table 5.1 lists the explicit functional requirements in this section.

49 The cryptographic module plays an important role in the enforcement of the TOE security policies. For this reason, the cryptographic related requirements contain more detail than other requirements, in terms of refinements, iterations, and explicitly stated requirements. Refer to section 1.3 to see the notation and formatting used in this profile.

**Table 5.1 - Explicitly Stated Functional Requirements**

| Explicit Component | Component Behavior Name |
|---|---|
| FCS_BCM_EXP.1 | Baseline Cryptographic Module |
| FCS_CKM_EXP.1 | Key Validation and Packaging |
| FCS_CKM_EXP.2 | Cryptographic Key Handling and Storage |
| FCS_COP_EXP.1 | Random Number Generation |
| FDP_ACF_US_INTERP_EXP.1 | Security Attribute Based Access Control |
| FDP_IFF_US_INTERP_EXP.2(1) | Hierarchical Security Attributes (for Mandatory Access Control) |
| FDP_IFF_US_INTERP_EXP.2(2) | Hierarchical Security Attributes (for Mandatory Integrity Control) |
| FIA_AFL_US_INTERP_EXP.1 | Authentication Failure Handling |
| FIA_USB_US_INTERP_EXP.1 | User-Subject Binding |
| FMT_MSA_EXP.1 | Rules for Management of Security Attributes |

## 5.1 Security Audit (FAU)

### 5.1.1 Security Audit Automatic Response (FAU_ARP)

#### 5.1.1.1 Security Alarms (FAU_ARP.1)

FAU_ARP.1.1 **Refinement:** The TSF shall **generate a warning for the authorized administrator** upon detection of a potential security violation.**1**

### 5.1.2 Security Audit Data Generation (FAU_GEN)

#### 5.1.2.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 **Refinement:** The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events **listed in Table 5.2**;

**c) All other security relevant auditable events** for the basic level of audit;

**d) Start-up and shutdown of the operating system; and**

**e) Uses of special permissions (e.g., by authorized administrators) that circumvent the access control policies.**

**Table 5.2 - Auditable Events**

| Requirement | Audit events prompted by requirement |
|---|---|
| Security Alarms (FAU_ARP.1) | • Actions taken due to imminent security violations |
| Audit Data Generation (FAU_GEN.1) | (none) |
| User Identity Association (FAU_GEN.2) | (none) |
| Potential Violation Analysis (FAU_SAA.1) | • Enabling and disabling of any of the analysis mechanisms.<br>• Automated responses provided by the tool. |
| Audit Review (FAU_SAR.1) | • Opening the audit trail. |
| Restricted Audit Review (FAU_SAR.2) | • Unsuccessful attempts to read information from the audit records |
| Selectable Audit Review (FAU_SAR.3) | (none) |
| Selective Audit (FAU_SEL.1) | • All modifications to the audit configuration that occur while the audit collection functions are operating. |
| Protected Audit Trail Storage (FAU_STG.1) | (none) |
| Prevention of Audit Data Loss (FAU_STG.4) | • Actions taken due to the audit storage failure. |
| Explicit: Baseline Cryptographic Module (FCS_BCM_EXP.1) | (none) |
| Cryptographic Key Generation (for symmetric keys) (FCS_CKM.1(1)) | • Success and failure of the activity.<br>• The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). |
| Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1(2)) | • Success and failure of the activity.<br>• The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). |
| Cryptographic Key Distribution (FCS_CKM.2) | • Success and failure of the activity.<br>• The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). |

| | |
|---|---|
| Cryptographic Key Destruction (FCS_CKM.4) | • Success and failure of the activity.<br>• The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). |
| Explicit: Key Validation and Packaging (FCS_CKM_EXP.1) | • Success and failure of the activity.<br>• The object attribute(s), and object value(s) excluding any sensitive information (e.g. keys). |
| Explicit: Cryptographic Key Handling and Storage (FCS_CKM_EXP.2) | • Success and failure of the activity.<br>• The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). |
| Cryptographic Operation (for data encryption/decryption services) (FCS_COP.1(1)) | • Success and failure, and the type of cryptographic operation.<br>• Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information |
| Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2)) | • Success and failure, and the type of cryptographic operation.<br>• Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information |
| Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3)) | • Success and failure, and the type of cryptographic operation.<br>• Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information |
| Cryptographic Operation (for cryptographic key exchange) (FCS_COP.1(4)) | • Success and failure, and the type of cryptographic operation.<br>• Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information |
| Explicit: Random Number Generation (FCS_COP_EXP.1) | (none) |
| Complete Access Control (FDP_ACC.2) | (none) |
| Security Attribute Based Access Control (FDP_ACF_US_INTERP_EXP.1) | • All requests to perform an operation on an object covered by the SFP. |
| Export of User Data With Security Attributes (FDP_ETC.2) | • All attempts to export information. |
| Complete Information flow control (for Mandatory Access Control Policy) (FDP_IFC.2(1)) | (none) |
| Complete Information flow control (for Mandatory Integrity Control Policy) (FDP_IFC.2(2)) | (none) |
| Hierarchical Security Attributes (for Mandatory Access Control) (FDP_IFF_US_INTERP_EXP.2(1)) | • All decisions on requests for information flow. |

| | |
|---|---|
| Hierarchical Security Attributes (for Mandatory Integrity Control) (FDP_IFF_US_INTERP_EXP.2(2)) | • All decisions on requests for information flow. |
| Limited Illicit information Flows (FDP_IFF.3) | • All decisions on requests for information flow.<br>• The use of identified illicit information flow channels. |
| Import of User Data Without Security Attributes (FDP_ITC.1) | • All attempts to import user data. |
| Import of User Data With Security Attributes (FDP_ITC.2) | • All attempts to import user data, including any security attributes. |
| Basic Internal Transfer Protection (FDP_ITT.1) | • All attempts to transfer user data, including identification of the protection method used and any error that occurred. |
| Full Residual Information Protection (FDP_RIP.2) | (none) |
| Authentication Failure Handling (FIA_AFL_US_INTERP_EXP.1) | • The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal). |
| User Attribute Definition (FIA_ATD.1) | (none) |
| Verification of Secrets (FIA_SOS.1) | • Rejection or acceptance by the TSF of any tested secret. |
| Timing of Authentication (FIA_UAU.1) | • All use of the authentication mechanism |
| Protected Authentication Feedback (FIA_UAU.7) | (none) |
| Timing of Identification (FIA_UID.1) | • All use of the user identification mechanism, including the user identity provided. |
| User-Subject Binding (FIA_USB_US_INTERP_EXP.1) | • Success and failure of binding of user security attributes to a subject (e.g. success and failure to create of a subject). |
| Management of Security Functions Behavior (FMT_MOF.1) | • All modifications in the behavior of the functions in the TSF. |
| Management of Security Attributes (for Discretionary Access Control) (FMT_MSA.1(1)) | • All modifications of the values of security attributes. |
| Management of Security Attributes (for Mandatory Access Control) (FMT_MSA.1(2)) | • All modifications of the values of security attributes. |
| Management of Security Attributes (for Mandatory Integrity Control) (FMT_MSA.1(3)) | • All modifications of the values of security attributes. |

| | |
|---|---|
| Secure Security Attributes (FMT_MSA.2) | • All offered and rejected values for a security attribute. |
| Static Attributes Initialization (FMT_MSA.3) | • Modifications of the default setting of permissive or restrictive rules.<br>• All modifications of the initial values of security attributes. |
| Explicit: Rules for Management of Security Attributes (FMT_MSA_EXP.1) | • All modifications of the values of security attributes. |
| Management of TSF Data (for general TSF data) (FMT_MTD.1(1)) | • All modifications of the values of TSF data, including audit data. |
| Management of TSF Data (for audit data) (FMT_MTD.1(2)) | • All modifications of the values of TSF data, including audit data. |
| Management of TSF Data (for user security attributes) (FMT_MTD.1(3)) | • All modifications of the values of TSF data, including audit data. |
| Management of TSF Data (for user security attributes, other than authentication data) (FMT_MTD.1(4)) | • All modifications of the values of TSF data, including audit data. |
| Management of TSF Data (for authentication data) (FMT_MTD.1(5)) | • All modifications of the values of TSF data, including audit data. |
| Management of TSF Data (for critical security parameters) (FMT_MTD.1(6)) | • All modifications of the values of TSF data, including audit data. |
| Revocation (to authorized administrators)(FMT_REV.1(1)) | • All attempts to revoke security attributes. |
| Revocation (to owners and authorized administrators) (FMT_REV.1(2)) | • All attempts to revoke security attributes. |
| Time-Limited Authorization (FMT_SAE.1) | • Specification of the expiration time for an attribute<br>• Action taken due to attribute expiration. |
| Security Roles (FMT_SMR.1) | • Modifications to the group of users that are part of a role. |
| Assuming Roles (FMT_SMR.3) | • Explicit requests to assume a role.<br>• Use of any function restricted to an authorized administrator role (identified in FMT_SMR.1). |
| Abstract Machine Testing (FPT_AMT.1) | • Execution of the tests of the underlying machine and the results of the tests. |
| Basic Internal TSF Data Transfer Protection (FPT_ITT.1) | (none) |
| TSF Data Integrity Monitoring (FPT_ITT.3) | • Detection of modification of TSF data |

| | |
|---|---|
| Manual Recovery (FPT_RCV.1) | • The fact that a failure or service discontinuity occurred.<br>• Resumption of the regular operation.<br>• Type of failure or service discontinuity |
| Non-Bypassability of the TSF (FPT_RVM.1) | (none) |
| SFP Domain Separation (FPT_SEP.2) | (none) |
| Reliable Time Stamps (FPT_STM.1) | • Changes to the time. |
| Inter-TSF Basic TSF Data Consistency (FPT_TDC.1) | • Successful use of TSF data consistency mechanisms.<br>• Use of TSF data consistency mechanisms. |
| Internal TSF Data Consistency (FPT_TRC.1) | • Restoring consistency upon reconnection.<br>• Detected inconsistency between TSF data. |
| TSF Testing (FPT_TST.1(1)) | • Execution of the TSF self tests and the results of the tests. |
| TSF Testing (for cryptography) (FPT_TST.1(2)) | • Execution of the self tests and the results of the tests. |
| TSF Testing (for key generation components) (FPT_TST.1(3)) | • Execution of the key generation component self tests and the results of the tests. |
| Maximum Quotas (for disk space and system memory) (FRU_RSA.1(1)) | • Rejection of allocation operation due to resource limits. |
| Maximum Quotas (for processing time) (FRU_RSA.1(2)) | • Rejection of allocation operation due to resource limits. |
| TSF-Initiated Session Locking (FTA_SSL.1) | • Locking of an interactive session by the session locking mechanism.<br>• Any attempts at unlocking of an interactive session. |
| User-Initiated Locking (FTA_SSL.2) | • Locking of an interactive session by the session locking mechanism.<br>• Any attempts at unlocking of an interactive session. |
| Default TOE Access Banners (FTA_TAB.1) | (none) |
| TOE Access History (FTA_TAH.1) | (none) |
| Trusted Path (FTP_TRP.1) | • All attempted uses of the trusted path functions.<br>• Identification of the user associated with all trusted path failures, if available. |

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,

- **the name, sensitivity label, and integrity label of the object;**
- **the sensitivity label and integrity label of the subject;**
- **for changes to TSF data, the new value (except authentication data and cleartext cryptographic variables, such as key variables, seed, etc.);**
- **for authentication attempts, the origin of the attempt (e.g., terminal identifier);**
- **for uses of a role, the type of role, and the origin of its request;**
- *[assignment: other audit relevant information]*.

#### 5.1.2.2 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

*Application Note: For failed login attempts no user association is required because the user is not under TSF control until after a successful identification/authentication, however, the origin of the attempt (e.g. terminal identification) is captured.*

### 5.1.3 Security Audit Analysis (FAU_SAA)

#### 5.1.3.1 Potential Violation Analysis (FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of *[assignment: subset of defined auditable events]* known to indicate a potential security violation;

b) *[assignment: any other rules]*.

### 5.1.4 Security Audit Review (FAU_SAR)

#### 5.1.4.1 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **authorized administrators** with the capability to read **all audit information** from the audit records.

FAU_SAR.1.2 **Refinement:** The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information **using a tool to access the audit trail.2**

*Application Note: It is expected (yet not necessary) that the tool satisfying this requirement will also satisfy the FAU_SAR.3 and FAU_SEL.1 requirements.*

#### 5.1.4.2 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

#### 5.1.4.3 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 **Refinement:** The TSF shall provide the ability to perform searches and sorting of audit data based on **the following attributes:**

**a) User identity;**

**b) Object identity;**

**c) Date of the event;**

**d) Time of the event;**

**e) Type of event;**

**f) Subject sensitivity label;**

**g) Object sensitivity label;**

**h) Subject integrity label;**

**i) Object integrity label; and**

**j)** ***[assignment: any additional attributes].***

### 5.1.5 Security Audit Event Selection (FAU_SEL)

#### 5.1.5.1 Selective Audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

**a)** object identity; user identity; host identity; event type;

**b) subject sensitivity label;**

**c) object sensitivity label;**

**d) subject integrity label;**

**e) object integrity label; and**

**f)** *[assignment: list of additional attributes that audit selectivity is based upon].*

### 5.1.6 Security Audit Event Storage (FAU_STG)

#### 5.1.6.1 Protected Audit Trail Storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

*Application Note: In order to reduce the performance impact of audit generation, audit records are often temporarily buffered in memory before being written to the disk. In such implementations, these buffered records will be lost if the operation of the TOE is interrupted by hardware or power failures. The developer should document the expected loss in such circumstances and show that it has been minimized.*

#### 5.1.6.2 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 **Refinement: When the audit trail becomes full,** the TSF shall **provide the authorized administrator the capability to** prevent auditable events, except those taken by the authorized **administrator (in the context of performing TOE maintenance)** and **generate an alarm to the authorized administrator.3**

# 5.2 Cryptographic Support (FCS)

## 5.2.1 Explicit: Baseline Cryptographic Module (FCS_BCM_EXP)

### 5.2.1.1 Explicit: Baseline Cryptographic Module (FCS_BCM_EXP.1)

**FCS_BCM_EXP.1.1** The cryptographic module shall comply with FIPS PUB 140-1.

**FCS_BCM_EXP.1.2** The cryptographic module implemented [selection: entirely in hardware shall have a minimum overall rating of FIPS PUB 140-1 Level 3, entirely in software shall have a minimum overall rating of FIPS PUB 140-1 Level 1, as a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-1 Level 1].

*Application Note: "Combination of hardware and software" means that some part of the cryptographic functionality will be implemented as a software component of the TSF. The combination of a cryptographic hardware module and a software device driver whose sole purpose is to communicate with the hardware module is considered a hardware module rather than a "combination of hardware and software".*

## 5.2.2 Cryptographic Key Management (FCS_CKM)

#### 5.2.2.1 Cryptographic Key Generation (for symmetric keys) (FCS_CKM.1(1))

FCS_CKM.1.1(1) **Refinement:** The TSF shall generate[9] **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **as follows**: **4** ***[selection:***

[9] This requirement applies strictly to **generation** of symmetric keys. **Validation** techniques for generated symmetric keys are discussed in FCS_CKM_EXP.1.1.

***(1) a hardware random number generator (RNG) as specified in FCS_COP_EXP.1, but with a NIST-approved hashing function (currently SHA-1) required for mixing, and/or***

***(2) a software random number generator (RNG) as specified in FCS_COP_EXP.1, and/or***

***(3) a key establishment scheme based upon public key cryptography using a software random number generator (RNG) as specified in FCS_COP_EXP.1, and/or a hardware random number generator (RNG) as specified in FCS_COP_EXP.1, but with a NIST-approved hashing function (currently SHA-1) required for mixing].***

that meets the following:

**a ) All cases: (i.e., any of the above)**

- **FIPS PUB 180-1, Secure Hash Algorithm;**
- **Sections from this PP: 5.6.9.2 TSF Testing (for cryptography) (FPT_TST.1(2)), 5.6.9.3 TSF Testing (for key generation component) (FPT_TST.1(3)), 5.2.3.5 Random Number Generation (FCS_COP_EXP.1), and 6.3 Development Documentation;**

**b) Case: Finite field-based key establishment schemes**

- **ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography;**

  *Application Note: For example, Diffie-Hellman-based schemes*

**c) Case: RSA-based key establishment schemes**

- **ANSI X9.44-2000, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Factoring-Based Cryptography; and**

**d) Case: Elliptic curve-based key establishment schemes**

- **ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography.**

### 5.2.2.2 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1(2))

FCS_CKM.1.1(2) **Refinement:** The TSF shall generate[10] **asymmetric**[11] cryptographic keys in accordance with a **domain parameter generator** and ***[selection:***

[10] This requirement applies strictly to **generation** of asymmetric keys. **Validation** techniques for generated asymmetric keys are discussed in FCS_CKM_EXP.1.2.

***(1) a random number generator and/or***

***(2) a prime number generator].***

that meet **the parameter generation criteria in** the following: **5**

**a) ANSI X9.80, Prime Number Generation, Primality Testing, and Primality Certificates, or FIPS PUB 186-2, Digital Signature Standard (prime number generation);**

**b) Sections from this PP: 5.6.9.2 TSF Testing (for cryptography) (FPT_TST.1(2)), 5.6.9.3 TSF Testing (for key generation component) (FPT_TST.1(3)), 5.2.3.5 Random Number Generation (FCS_COP_EXP.1), and 6.3 Development Documentation;**

**c) Case: For domain parameters used in finite field-based key establishment schemes**

- **ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography;**

  *Application Note: For example, Diffie-Hellman-based schemes*

**d) Case: For domain parameters used in RSA-based key establishment schemes**

- **ANSI X9.44-2000, Public Key Cryptography for the Financial Services Industry: Key Agreement and Transport Using Factoring-Based Cryptography; and**

**e) Case: For domain parameters used in elliptic curve-based key establishment schemes**

- **ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography.**

### 5.2.2.3 Cryptographic Key Distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***[selection: Manual (Physical) Method, Automated (Electronic) Method, Manual Method and Automated Method]*** that meets the following:

**a) Manual (Physical) Methods:**

**• The TSF shall manually distribute (establish) symmetric key in accordance with a NIST-approved cryptographic key distribution method specified by FIPS PUB 140-1 and FIPS PUB 171[12] (Key Management using ANSI X9.17).**

---

[11] These are the keys/parameters (e.g., the public/private key pairs) underlying a public key-based key establishment scheme, not the session keys established by such schemes.

[12] For purposes of interpreting this standard, only Triple Data Encryption Algorithm (TDEA) with 168 bits of key shall be applied (DES is not acceptable for meeting this requirement. Eventual migration to AES is expected.).

**• The TSF shall manually distribute (establish) asymmetric public key material (certificates and/or keys) in accordance with NIAP-certified DoD PKI for public key distribution using NSA-approved certificate schemes[13] with hardware tokens for protection of private keys that meet the following:**

1) **PKI Roadmap for the DoD,**
2) **DoD X.509 Certificate Policy,**
3) **PKSC#8 (Private-Key Information Syntax Standard),**
4) **PKSC#12 (Personal Information Exchange Syntax),**
5) **PKSC#5 (Password-Based Encryption Standard), and**
6) **PKSC#11 (Cryptographic Token Interface Standard).**

**• The TSF shall manually distribute (establish) asymmetric (public) key material (certificates and/or keys) in accordance with NIAP-certified DoD PKI for public key distribution using NSA-approved certificate schemes[14] for protection of public keys that meet the following:**

1. **PKI Roadmap for the DoD,**
2. **DoD X.509 Certificate Policy,**
3. **PKSC#12 (Personal Information Exchange Syntax),**

**b) Automated (Electronic) Methods:**

**• The TSF shall automatically distribute (establish) symmetric key in accordance with a NIST-approved cryptographic key distribution method specified by FIPS PUB 140-1 and FIPS PUB 171[15] (Key Management Using ANSI X9.17).**

**• The TSF shall automatically distribute public asymmetric (public) key material (certificates and/or keys) in accordance with NIAP-certified DoD PKI for public key distribution using NSA-approved certificate schemes[16] that meet the following:**

1. **PKI Roadmap for the DoD,**

[13] DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes with hardware tokens for protection of private key is approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

[14] DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes are approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

[15] For purposes of interpreting this standard, only TDEA with 168 bits of key shall be applied (DES is not acceptable for meeting this requirement. Eventual migration to AES is expected.).

[16] DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes are approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

2. **DoD X.509 Certificate Policy,**
3. **PKSC#12 (Personal Information Exchange Syntax),**

**• The TSF shall not automatically distribute private asymmetric (public) key material.**

#### 5.2.2.4 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1: **Refinement:** The TSF shall destroy cryptographic keys in accordance with a **cryptographic key destruction method** that meets the following:**6**

**a) FIPS PUB 140-1;**

**b) Zeroization of all plaintext cryptographic keys and all other critical security parameters shall be immediate and complete; and**

**c) For embedded cryptographic modules, the destruction shall be executed by overwriting the key/critical security parameter storage area three or more times with an alternating pattern.**

### 5.2.2.5 Explicit: Key Validation and Packaging (FCS_CKM_EXP.1)

**FCS_CKM_EXP.1.1:** The TSF shall apply validation techniques (e.g., parity bits or checkwords) to each generated symmetric key in accordance with:

a) FIPS PUB 46-3 (Data Encryption Standard (DES)), and

b) FIPS PUB 171[17] (Key Management Using ANSI X9.17).

**FCS_CKM_EXP.1.2:** The TSF shall apply validation techniques to generated asymmetric keys in accordance with the standards corresponding to the generation technique as called out in FCS_CKM.1.1(2).

**FCS_CKM_EXP.1.3:** Any public key certificates generated by the TSF shall be in accordance with NIAP-certified NSA-approved certificate schemes[18].

### 5.2.2.6 Explicit: Cryptographic Key Handling and Storage (FCS_CKM_EXP.2)

**FCS_CKM_EXP.2.1:** The TSF shall perform key entry and output in accordance with FIPS PUB 140-1, Level 3.

[17] For purposes of interpreting this standard, only TDEA with 168 bits of key shall be applied (DES is not acceptable for meeting this requirement. Eventual migration to AES is expected.).

[18] DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes with hardware tokens for protection of private key are approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

**FCS_CKM_EXP.2.2:** The TSF shall provide a means to ensure that keys are associated with the correct entities (i.e., person, group, or process) to which the keys are assigned.

**FCS_CKM_EXP.2.3:** The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

*Application Note: A parity check is an example of a key error detection check.*

**FCS_CKM_EXP.2.4:** The TSF shall encrypt or split secret and private keys when not in use.

**FCS_CKM_EXP.2.5:** The TSF shall overwrite each intermediate storage area for plaintext key/critical security parameters three or more times with an alternating pattern upon the transfer of the key/critical security parameter to another location.

*Application Note: This is related to the elimination of internal, temporary copies of keys created during processing, not to the total destruction of a key from the TOE which is discussed under Key Destruction.*

**FCS_CKM_EXP.2.6:** The TSF shall perform any key archiving in accordance with a NIST-approved key archiving method that meets the following:

**a) FIPS PUB 140-1 (Key Archiving section).**

**b) Archiving of signature keys is prohibited.**

## 5.2.3 Cryptographic Operation (FCS_COP)

### 5.2.3.1 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1.1(1) **Refinement:** The TSF shall perform **data encryption/decryption services** in accordance with a **NIST-approved** cryptographic algorithm **Triple Data Encryption Algorithm[19] (TDEA)** and cryptographic key size **of 168 bits (three independent keys)** that meets the following*: **1***

**a) FIPS PUB 140-1**

**b) FIPS PUB 46-3, and**

**c) ANSI X9.52 (Triple Data Encryption Algorithm Modes of Operation).**

### 5.2.3.2 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with the **NIST-approved digital signature** algorithm ***[selection:***

[19] The Advanced Encryption Standard (AES) employing key lengths of 128 bits or greater and meeting NIST-approved AES standards will be required when AES is fully established.

***(1) Digital Signature Algorithm (DSA) with a key size (modulus) greater than 3000 bits ,***

***(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) greater than 3000 bits, or***

***(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]***

that meets the following:**8**

**a) FIPS PUB 186-2, Digital Signature Standard, if using the Digital Signature Algorithm;**

**b) ANSI X9.31, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), if using the RSA Digital Signature Algorithm;**

**c) ANSI X9.62, Public Key Cryptography for the Financial Services Industry: Elliptic Curve Digital Signature Algorithm (ECDSA), if using the elliptic curve digital signature algorithm.**

5.2.3.3 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1.1(3) **Refinement:** The TSF shall perform **cryptographic hashing services** in accordance with the **NIST-approved hash** algorithm **Secure Hash Algorithm 1 (SHA-1)** and **hash size of 160-bit[20] message digest** that meets the following**: FIPS PUB 180-1.9**

5.2.3.4 Cryptographic Operation (for cryptographic key exchange) (FCS_COP.1(4))

FCS_COP.1.1(4) **Refinement:** The TSF shall perform **cryptographic key exchange services** in accordance with the **NIST-approved key exchange** algorithm ***[selection:***

1. ***Diffie-Hellman Algorithm and cryptographic key sizes greater than 3000 bits,***
2. ***RSA Algorithm and cryptographic key size greater than 3000 bits, or***
3. ***Elliptic Curve Key Exchange Algorithm (ECKEA) and cryptographic key sizes of 256 bits or greater]***

that meet the following:**10**

**a) ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, if a finite-field-based scheme is used;**

*Application Note: For example, Diffie-Hellman-based schemes*

[20] Future migration to incorporate stronger cryptographic hashing services (i.e., with a digest corresponding to double the system encryption key strength) will be required when such NIST standards are established.

**b) ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Elliptic Curve Cryptography, if an elliptic-curved-based scheme is used; and**

**c) ANSI X9.44-2000, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Factoring-Based Cryptography, if an RSA-based scheme is used.**

*Application Note: An authentication mechanism on the keying material is recommended. In addition, repeated generation of the shared secrets should be avoided. As an example, the MQV schemes described in the above standards address these issues.*

#### 5.2.3.5 Explicit: Random Number Generation (FCS_COP_EXP.1)

**FCS_COP_EXP.1.1** The TSF shall perform all random number generation (RNG) services in accordance with ***[selection:***

***(1) multiple independent hardware-generated inputs combined with a mixing function, or***

*Application Note: A NIST-approved hashing function is recommended for the mixing function in hardware based RNGs.*

***(2) multiple independent software-generated inputs combined with a NIST-approved hashing function (currently SHA-1), or***

*Application Note: A NIST-approved hashing function is required for the mixing function in software based RNGs.*

***(3) a combination of multiple independent hardware-generated inputs combined with a mixing function and multiple independent software-generated inputs combined with a NIST-approved hashing function (currently SHA-1)]***

that meet the following:

a) FIPS PUB 180-1, when using a NIST-approved hashing function as the mixing function,

b) NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications;

*Application Note: Successful completion and documentation of these tests during the TOE development helps to demonstrate the random number generator design is rigorous. There exists a NIST toolbox for running these tests.*

c) All the RNG/PRNG self-tests of FIPS PUB 140-1, Level 4,

d) The augmented tests and self-test requirements in this PP: TSF Self Testing, and

e) RNG/PRNG design and test documentation consistent with that required in this PP for other subsystems: Development Documentation (Section 6.3)

**FCS_COP_EXP.1.2** The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

*Application Note: The RNG/PRNG should be resistant to manipulation or analysis of its sources, or any attempts to predictably influence its states. Three examples of very different approaches the TSF might pursue to address this include: a) identifying the fact that physical security must be applied by the product embedding the OS (i.e., deferring the requirement), b) applying checksums over the sources, or c) designing and implementing the TSF RNG with a concept similar to a keyed hash (e.g., where periodically the initial state of the hash is changed unpredictably and each change is protected as when provided on a tamper-protected token, or in a secure area of memory.*

# 5.3 User Data Protection (FDP)

## 5.3.1 Access Control Policy (FDP_ACC)

### 5.3.1.1 Complete Access Control (FDP_ACC.2)

FDP_ACC.2.1 **Refinement:** The TSF shall enforce the **Discretionary Access Control policy** on *[assignment: list of all subjects and **all named** objects]* and all operations among them.**11**

*Application Note: The DAC policy does not cover local public objects.*

FDP_ACC.2.2 **Refinement:** The TSF shall ensure that all operations between any subject and any **named** object are covered by **the Discretionary Access Control policy**.**12**

## 5.3.2 Access Control Functions (FDP_ACF)

### 5.3.2.1 Explicit: Security Attribute Based Access Control (FDP_ACF_US_INTERP_EXP.1)

**FDP_ACF_US_INTERP_EXP.1.1 Refinement:** The TSF shall enforce the **Discretionary Access Control policy** to **named** objects based on the following types of subject and object security attributes[21]:

**a) The authorized user identity and group membership(s) associated with a subject; and**

**b) The access control attributes associated with a named object[22] with:**

**• the ability to associate allowed and denied operations with authorized user identities;**

**• the ability to associate allowed and denied operations with group identities; and**

[21] US Common Criteria Interpretation #0353: "Association of Access Control Attributes with Subjects and Objects" (http://www.radium.ncsc.mil/tpep/library/interps/0353.html).

[22] In accordance with FDP_ACC.2.1, this policy applies to remote public objects but not to local public objects.

**• defaults for allowed or denied operations.**

*Application Note: This requirement is worded to include only implementations where access control attributes are associated with objects rather than subjects. This implementation becomes critical when satisfying FMT_MTD.1.1(3) and FMT_REV.1.1(1) .*

FDP_ACF_US_INTERP_EXP.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among subjects and **named** objects is allowed:[13]

**a) The TSF shall define and control access between subjects and named objects in the system.**

**b) The enforcement mechanism (e.g., access control lists) shall allow authorized users to specify and control sharing of named objects by user identities, or group identities, or by both, and shall provide controls to limit propagation of access rights.**

**c) The discretionary access control mechanism shall, either by explicit authorized user action or by default, provide that named objects are protected from unauthorized access.**

**d) These access controls shall be capable of including or excluding access to the granularity of a single user.**

**e) Access permission to a named object by users not already possessing access permission shall only be assigned by authorized users.**

**f) Access control entries shall be interpreted such that the one with the most specific identity takes precedence.**

FDP_ACF_US_INTERP_EXP.1.3 **Refinement:** The TSF shall explicitly authorize access of subjects to **named** objects based on the following additional rules:

**a) Authorized administrators must follow the above-stated Discretionary Access Control policy, except after taking the following specific actions: *[assignment: list of specific actions]*.**

b) *[assignment: other rules, based on security attributes, that explicitly authorize access of subjects to* **named** *objects]*.

*Application Note: This element allows specifications of additional rules for authorized administrators to bypass the Discretionary Access Control policy for system management or maintenance (e.g., system backup).*

FDP_ACF_US_INTERP_EXP.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to **named** objects based on the following rules:

a) If a given identity is specified more than once in the access control information for a given named object, then the most restrictive access will be granted.

b) *[assignment: rules, based on security attributes, that explicitly deny access of subjects to* ***named*** *objects]*.

## 5.3.3 Export to Outside TSF Control (FDP_ETC)

### 5.3.3.1 Export of User Data With Security Attributes (FDP_ETC.2)

FDP_ETC.2.1 The TSF shall enforce the **Mandatory Access Control and Mandatory Integrity Control policies** when exporting user data, controlled under the SFPs, outside of the TSC.

*Application Note: For this family (FDP_ETC) the term "security attributes" refers only to the sensitivity and integrity labels of subject and objects.*

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC:

**a) When data is exported in hardcopy form each page shall be marked with a printed representation of the "least upper bound" sensitivity label of all data exported to the page. By default this marking shall appear on both the top and bottom of each printed page.**

**b) If a device capable of maintaining data security attributes, the security attributes shall be exported with the data.**

**c) *[Assignment: Any additional rules that control the export of information from the TSC and their corresponding security attributes. In all cases the TOE must export the security attributes with the corresponding information]***

## 5.3.4 Information Flow Control Policy (FDP_IFC)

### 5.3.4.1 Complete Information flow control (for Mandatory Access Control Policy) (FDP_IFC.2(1))

FDP_IFC.2.1(1) **Refinement:** The TSF shall enforce the **Mandatory Access Control policy** on ***[assignment: list of all subjects and all objects]***, and all operations that cause information to flow **among them**.[14]

*Application Note: In most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST. The ST author must also explicitly list the objects that exist in the TOE; this list must include storage objects (data storage resources, input/output devices, etc.) as well as named objects, which are used to share information among subjects acting on the behalf of different users, and for which access to the object can be specified by a name or other identity (such as files or their equivalents). The operations, listed in the ST, among subjects and objects must explicitly define all relationships between subjects and objects in the TOE, and must be consistent with the list of objects defined in the earlier assignment.*

*Application Note: The MAC policy covers all subjects and all objects. The list of objects must include object attributes that are themselves objects (such as filenames) because they can be manipulated by a user.*

FDP_IFC.2.2(1) **Refinement:** The TSF shall ensure that all operations that cause any information in the TSC to flow **among subjects and objects** in the TSC are covered by the **MAC** SFP.**15**

#### 5.3.4.2 Complete Information flow control(for Mandatory Integrity Control Policy) (FDP_IFC.2(2))

FDP_IFC.2.1(2) **Refinement:** The TSF shall enforce the **Mandatory Integrity Control policy** on ***[assignment: list of all subjects and objects]***, and all operations that cause that information to flow **among them**.**16**

*Application Note: The Mandatory Integrity Control policy is based upon trustworthiness: subjects with a low degree of trustworthiness cannot change data of a higher degree of trustworthiness. A subject with a high degree of trustworthiness can not be forced to rely on data of a low degree of trustworthiness.*

FDP_IFC.2.2(2) **Refinement:** The TSF shall ensure that all operations that cause any information in the TSC to flow **among subjects and objects** in the TSC are covered by the **MIC** SFP.**17**

## 5.3.5 Information Flow Control Functions (FDP_IFF)

### 5.3.5.1 Explicit: Hierarchical Security Attributes (for Mandatory Access Control) (FDP_IFF_US_INTERP_EXP.2(1))

**FDP_IFF_US_INTERP_EXP.2.1(1) Refinement:** The TSF shall enforce the **Mandatory Access Control policy** based on the following types of subjects, **objects,** and security attributes[23]**18**:

**a)** ***[Assignment: list of all subjects]***

**b) the sensitivity label of the subject consisting of at least 8 site definable hierarchical levels and a set of 60 site definable non-hierarchical categories;**

*Application Note: The implementation of sensitivity labels does not need to store labels in a format that has the components of the label explicitly instantiated, but may use some form of tag which maps to a level and category set.*

**c)** ***[Assignment: list of all objects]***

**d) the sensitivity label of the object consisting of at least 8 site definable hierarchical levels and a set of 60 site definable non-hierarchical categories;**

**e)** ***[Assignment: list of any additional security attributes]*.**

[23] US Common Criteria Interpretation #0354 :"Association of Information Flow Attributes with Subjects and Information"

*Application Note: For this family (FDP_IFF) the term "security attributes" refers only to the sensitivity labels of subject and objects.*

FDP_IFF_US_INTERP_EXP.2.2(1) **Refinement:** The TSF shall permit an information flow **among subjects and objects** based on the following rules:[19]

**a) If the sensitivity label of the subject is greater than (see FDP_IFF_US_INTERP_EXP.2.7) or equal to the sensitivity label of the object, then the flow of information from the object to the subject is permitted (a read operation);**

**b) If the sensitivity label of the object is greater than or equal to the sensitivity label of the subject; then the flow of information from the subject to the object is permitted (a write operation);**

*Application Note: where the label of the object is greater than the label of the subject, this is a blind append (i.e., write does not imply a read).*

**c) If the information flow is between objects, the sensitivity label of the destination object must be greater than (see FDP_IFF_US_INTERP_EXP.2.7) or equal to the sensitivity label of the source object.**

FDP_IFF_US_INTERP_EXP.2.3(1) **Refinement:** The TSF shall **provide authorized administrators with a MAC-exempt capability by *[assignment: list of means of invoking MAC-exempt rules]*.**[20]

FDP_IFF_US_INTERP_EXP.2.4(1) The TSF shall provide the following: ***[assignment: list of administrator actions requiring MAC-exemption]***.

FDP_IFF_US_INTERP_EXP.2.5(1) The TSF shall explicitly authorize an information flow based on the following rules: *[assignment: rules based on security attributes that explicitly authorize information flows]*.

*Application Note: These rules regulate the behavior for each of the roles identified under FMT_SMR.*

FDP_IFF_US_INTERP_EXP.2.6(1) The TSF shall explicitly deny an information flow based on the following rules*: [assignment: rules based on security attributes that explicitly deny information flows]*.

FDP_IFF_US_INTERP_EXP.2.7(1) **Refinement:** The TSF shall enforce the following relationships for any two valid **MAC** security attributes:[21]

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;

**1. Sensitivity labels are equal if the hierarchical level of both labels are equal and the non-hierarchically category sets are equivalent;**

**2. Sensitivity label A is greater than sensitivity label B if the hierarchical level of A is greater than or equal to the hierarchical level of B, and the non-hierarchical**

**category set of A is equal to or a superset of the non-hierarchical category set of B.**

**3. Sensitivity labels are incomparable if they are not equal and neither label is greater than the other.**

b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and

c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes**.**

#### 5.3.5.2 Explicit: Hierarchical Security Attributes (for Mandatory Integrity Control) (FDP_IFF_US_INTERP_EXP.2(2))

FDP_IFF_US_INTERP_EXP.2.1(2) **Refinement:** The TSF shall enforce the **Mandatory Integrity Control policy** based on the following types of subjects, **objects,** and security attributes:[22]

***a) [Assignment: list of all subjects];***

**b) the integrity label of the subject;**

***c) [Assignment: list of all objects];***

**d) the integrity label of the object containing the information;**

***e) [Assignment: any additional security attributes].***

*Application Note: Example of such integrity labels are those cited in the Biba Integrity policy.*

*Application Note: For this family (FDP_IFF) the term "security attributes" refers only to the sensitivity labels of subject and objects.*

FDP_IFF_US_INTERP_EXP.2.2(2) **Refinement:** The TSF shall permit an information flow **among subjects and objects** based on the following rules:[23]

**a) If the integrity label of the subject is greater than or equal to the integrity label of the object, then a write (the flow of information from the subject to the object) is permitted;**

**b) If the integrity label of the object is greater than or equal to the integrity label of the subject; then a read (the flow of information from the object to the subject) is permitted;**

**c) If the information flow is between objects, the integrity label of the source object must be greater than or equal to the sensitivity label of the destination object.**

FDP_IFF_US_INTERP_EXP.2.3(2) **Refinement:** The TSF shall **provide authorized administrators with a MIC-exempt capability by *[assignment: list of means of invoking MIC-exempt rules]*.**[24]

FDP_IFF_US_INTERP_EXP.2.4(2) The TSF shall provide the following: ***[assignment: list of administrator actions requiring MIC-exemption]***.

FDP_IFF_US_INTERP_EXP.2.5(2) The TSF shall explicitly authorize an information flow based on the following rules: *[assignment: rules, based on security attributes, that explicitly authorize information flows].*

*Application Note: These rules regulate the behavior for each of the roles identified under FMT_SMR.*

FDP_IFF_US_INTERP_EXP.2.6(2) The TSF shall explicitly deny an information flow based on the following rules*: [assignment: rules, based on security attributes, that explicitly deny information flows].*

FDP_IFF_US_INTERP_EXP.2.7(2) **Refinement:** The TSF shall enforce the following relationships for any two valid **MIC** security attributes:[25]

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;

b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and

c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

#### 5.3.5.3 Limited Illicit Information Flows (FDP_IFF.3)

FDP_IFF.3.1 **Refinement:** The TSF shall enforce the **Mandatory Access Control policy** to **ensure that no illicit information flows exist which cross the cryptographic boundaries**.[26]

*Application Note: The analysis need not be performed on data other than that composing cryptographic keys and other critical security parameters. The analysis for such flows is also covered by the AVA_CCA requirements.*

## 5.3.6 Import From Outside TSF Control (FDP_ITC)

#### 5.3.6.1 Import of User Data Without Security Attributes (FDP_ITC.1)

FDP_ITC.1.1 **Refinement:** The TSF shall enforce the **Mandatory Access Control and Mandatory Integrity Control policies** when importing **any unlabeled** user data, **or non-validated labeled user data** controlled under the SFP, from outside the TSC.

*Application Note: The "label" is the security attributes associated with the data. Validated labels are recognized labels that are cryptographically verified and originate from a source deemed trustworthy (e.g., by the authorized administrator).*

*Application Note: For this family (FDP_ITC) the term "security attributes" refers only to the sensitivity labels of subject and objects.*

FDP_ITC.1.2 **Refinement:** The TSF shall ignore any security attributes associated with the **non-validated** user data when imported from outside the TSC.

FDP_ITC.1.3 **Refinement:** The TSF shall enforce the following rules when importing **unlabeled or non-validated** user data controlled under the SFP from outside the TSC:

**a) When importing data that has no validated MAC label (see FDP_ITC.2.5), the TSF shall allow the authorized administrator to specify that the data is to be labeled with (1) the label of the subject importing the data, (2) the label of the device by which the data is imported, or (3) the highest MAC label of data processed by the TOE;**

**b) When importing data that has no validated integrity label (see FDP_ITC.2.5), the TSF shall allow the authorized administrator to specify that the data is to be labeled with (1) the label of the subject importing the data, (2) the label of the device by which the data is imported, or (3) the lowest integrity label of data processed by the TOE;**

**c) When importing data, the data is given the Discretionary Access Control attributes, the data is to be given the Discretionary Access Control attributes of the importer of the data;**

*d) [Assignment: any additional importation control rules].*

*Application Note: The ST author must explicitly state the rules under which authorized users can designate the security attributes of the mechanisms, or devices, used to import data without security attributes; and any attribute change must be audited. The ST author must also make it clear that mechanisms, or devices, used to import data without security attributes cannot also be used to import data with security attributes unless this change in state can only be done manually and is audited.*

### 5.3.6.2 Import of User Data With Security Attributes (FDP_ITC.2)

FDP_ITC.2.1 **Refinement:** The TSF shall enforce the **Mandatory Access Control and Mandatory Integrity Control policies,** when importing **validated labeled** user data, controlled under the SFP, from outside the TSC.

*Application Note: The "label" is the security attributes associated with the data. Validated labels are recognized labels that are cryptographically verified and originate from a source deemed trustworthy (e.g., by the authorized administrator).*

FDP_ITC.2.2 **Refinement:** The TSF shall use the security attributes associated with the imported **validated labeled** user data.

FDP_ITC.2.3 **Refinement:** The TSF shall ensure that the protocol used provides for the **correct** unambiguous association between the **imported security attributes** and the **imported** user data.**27**

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:

**a) A cryptographic mechanism (e.g., cryptographic signature) shall be used to validate the security attributes.**

**b) If the validation mechanism fails, the data shall be treated as if it had no security attributes.**

**Application Note: The process for treating data with no security attributes is defined in FDP_ITC.1.c) If the data contains security attributes that are not recognized by the TOE, yet the TOE has a means of obtaining the security attributes' scheme used by the origin of the data, then the TOE must assign the data its own representation of the equivalent security attributes.**

**d) If the data contains any security attributes that are not recognized by the TOE, and the TOE does not have a means of obtaining the security attributes' scheme used by the origin of the data, then those security attributes must be rejected, while recognized security attributes may still be accepted;**

**Application Note: The process for treating data with no security attributes is defined in FDP_ITC.1.e) If the source of the imported data is not considered trustworthy according to the Organizational Security Policy (e.g., via a certificate mechanism), then the data must be treated as if it had no integrity label.**

**Application Note: The process for treating data with no security attributes is defined in FDP_ITC.1.f) *[Assignment: any additional importation control rules]*.**

*Application Note: The ST must describe the labeling system that is used by the TOE, so that integrators can avoid interconnecting TOEs whose bit-pattern representations for labels are in conflict. If the TOE includes a mechanism for countering such potential conflicts (e.g., a label representation translator, a means of accepting labels only from certain locations, etc), the rules enforced by such a mechanism should be included in the rules of FDP_ITC.2.5.*

## 5.3.7 Internal TOE Transfer (FDP_ITT)

### 5.3.7.1 Basic Internal Transfer Protection (FDP_ITT.1)

FDP_ITT.1.1 The TSF shall enforce the **Discretionary Access Control, Mandatory Access Control, and Mandatory Integrity Control policies** to prevent the disclosure **and** modification of user data when it is transmitted between physically-separated parts of the TOE.

*Application Note: If not physically protected (see A.PHYSICAL), other protection mechanisms that prevent disclosure and modification of user data include link encryption, application-level protection (SHTTP), or some other mechanism described in the ST.*

### 5.3.8 Residual Information Protection (FDP_RIP)

#### 5.3.8.1 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1 **Refinement:** The TSF shall ensure that any previous information content of a resource is made unavailable upon the *[selection: allocation of the resource to, deallocation of the resource from]* all objects **other than those associated with cryptographic keys and critical security parameters as described in FCS_CKM.4.1 and FCS_CKM_EXP.2.5**.

*Application Note: This requirement applies to all resources governed by or used by the TSF; it includes resources used to store data and attributes. It also includes the encrypted representation of information.*

*Application Note: Clearing the content of resources on deallocation is sufficient to satisfy this requirement, provided that unallocated resources will not accumulate new information until they are allocated again.*

## 5.4 Identification and Authentication (FIA)

### 5.4.1 Authentication Failures (FIA_AFL)

#### 5.4.1.1 Explicit: Authentication Failure Handling (FIA_AFL_US_INTERP_EXP.1)

**FIA_AFL_US_INTERP_EXP.1.1 Refinement:** The TSF shall detect when an authorized administrator configurable **positive** integer of unsuccessful authentication attempts occur related to **any authorized user authentication process**.[24]

FIA_AFL_US_INTERP_EXP.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:

**a) For all administrator accounts, disable the account for an authorized administrator configurable time period;**

**b) For all other accounts, disable the user logon account until it is re-enabled by the authorized administrator.**

**c) For all disabled accounts, respond with an "account disabled" message without attempting any type of authentication.**

### 5.4.2 User Attribute Definition (FIA_ATD)

#### 5.4.2.1 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

**a) Unique Identifier;**

[24] US Common Criteria Interpretation #0377 :"Settable Failure Limits are Permitted"

**b) Group Memberships;**

**c) Authentication Data;**

**d) Security level;**

**e) Integrity Level;**

**f) Security-relevant Roles (see FMT_MOF.1); and**

***g) [Assignment: Any security attributes related to cryptographic function (e.g., certificate used to represent the user, key used to encrypt data on behalf of the user)].***

***h) [Assignment: Any other security attributes (e.g., privilege)].***

*Application Note: Group membership may be expressed in a number of ways: a list per user specifying to which groups the user belongs, a list per group which includes which users are members, or implicit association between certain user identities and certain groups.*

*Application Note: A TOE may have two forms of user and group identities, a text form and a numeric form, which have a unique mapping between the representations. It is possible that the notion of privilege is tied to the security-relevant roles (item f).*

## 5.4.3 Specification of Secrets (FIA_SOS)

### 5.4.3.1 Verification of Secrets (FIA_SOS.1)

FIA_SOS.1.1 **Refinement:** The TSF shall provide a mechanism to verify that secrets meet **the following:**

**a) For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in $2.5 \times 10^{14}$;**

*Application Note: This can be achieved with a password greater than eight characters, assuming an alphabet of 60 characters.*

**b) The authentication mechanism must provide a delay between attempts, such that there can be no more than ten attempts per minute; and**

**c) Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.**

*Application Note: The ST must specify the method of authentication. Where authentication is provided by a password mechanism, the ST shows that the restrictions upon passwords (length, alphabet, and other characteristics) result in a password space conforming to item (a) above, as well as characterize the delay to show conformance to item (b) above. Where authentication is provided by a mechanism other than passwords, the ST shows the authentication method has a low probability that authentication data can be forged or guessed.*

## 5.4.4 User Authentication (FIA_UAU)

### 5.4.4.1 Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 **Refinement:** The TSF shall allow **read access to *[assignment: list of public objects]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 **Refinement:** The TSF shall require each user to be successfully authenticated **(i.e., an exact match between the user's entered data and the stored TSF authentication data)** before allowing any other TSF-mediated actions on behalf of that user.

*Application Note: The entire entered user's authentication data must exactly match the entire stored data. No other parameters such as length of password should be used to short-circuit the authentication verification.*

### 5.4.4.2 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the user while the authentication is in progress.

*Application Note: "Obscured feedback" implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user, which may provide any indication of the authentication data.*

## 5.4.5 User Identification (FIA_UID)

### 5.4.5.1 Timing of Identification (FIA_UID.1)

FIA_UID.1.1 **Refinement:** The TSF shall allow **read access to *[assignment: list of public objects]*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

## 5.4.6 User-Subject Binding (FIA_USB)

### 5.4.6.1 Explicit: User-Subject Binding (FIA_USB_US_INTERP_EXP.1)

**FIA_USB_US_INTERP_EXP.1.1** The TSF shall associate the following user security attributes with subjects acting on behalf of that user:[25]

**a) The user unique identity that is associated with auditable events;**

[25] US Common Criteria Interpretation #0351 "Attributes To Be Bound Should Be Specified".

**b) The user identity or identities that are used to enforce the Discretionary Access Control Policy;**

*Application Note: The DAC and audit policies require that each subject acting on behalf of a user has a user identity associated with the subject. While this identity is typically the one used at the time of identification to the system, the DAC policy enforced by the TSF may include provisions for making access decisions based upon a different user identity, such as the "set user ID (su)" command in UNIX.*

**c) The group identity or identities that are used to enforce the Discretionary Access Control Policy;**

**d) The user security level that is used to enforce the Mandatory Access Control policy;**

**e) The user integrity level that is used to enforce the Mandatory Integrity Control policy;**

***f) [Assignment: other list of user security attributes related to cryptographic function (e.g., certificate used to represent the user, key used to encrypt data on behalf of the user)].***

***g) [Assignment: other list of user security attributes to be bound (e.g., privilege)].***

*Application Note: The attributes listed in FIA_USB_US_INTERP_EXP.1 should be comparable to those listed in FIA_ATD.1. For example, the user's current sensitivity level (FIA_USB_US_INTERP_EXP.1 item d) should be within the set of the user's clearances (FIA_ATD.1 item d).*

# 5.5 Security Management (FMT)

## 5.5.1 Management of Functions in TSF (FMT_MOF)

### 5.5.1.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1(1) The TSF shall restrict the ability to determine the behavior of, disable, enable, and modify the behavior of the functions **related to the selection of which events are to be audited (see FAU_SEL.1.1)** to **the authorized administrators.**

FMT_MOF.1.1(2) The TSF shall restrict the ability to enable the functions **associated with changing the values of user authentication data** to **authorized administrators and users authorized to modify their own authentication data.**

## 5.5.2 Management of Security Attributes (FMT_MSA)

### 5.5.2.1 Management of Security Attributes (for Discretionary Access Control) (FMT_MSA.1(1))

FMT_MSA.1.1(1) **Refinement:** The TSF shall enforce the **Discretionary Access Control policy** to restrict the ability to query **and change** the **value of**

**the object** security attributes **to authorized administrators and owners of the object.**[28]

#### 5.5.2.2 Management of Security Attributes (for Mandatory Access Control) (FMT_MSA.1(2))

FMT_MSA.1.1(2) The TSF shall enforce the **Mandatory Access Control policy** to restrict the ability to **change** the **value of the sensitivity label associated with an object** to **authorized administrators**.[29]

#### 5.5.2.3 Management of Security Attributes (for Mandatory Integrity Control) (FMT_MSA.1(3))

FMT_MSA.1.1(3) The TSF shall enforce the **Mandatory Integrity Control policy** to restrict the ability to **change** the **value of the integrity label associated with an object** to **authorized administrators**.[30]

#### 5.5.2.4 Secure Security Attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

*Application Note: "Secure values" are those defined in the associated guidance documentation. The identity attributes are listed in FDP_ACF_US_INTERP_EXP.1, FDP_IFC.2, and FIA_ATD.1.*

#### 5.5.2.5 Static Attributes Initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Discretionary Access Control policy** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **authorized administrator** to specify alternative initial values to override the default values when an object or information is created.

*Application Note: The TOE must provide protection by default for all objects at creation time. This may be accomplished through the enforcement of a restrictive default access on objects, or through requiring the user to explicitly specify the desired access controls upon the object at its creation, provided that there is no window of vulnerability through which unauthorized access may be gained to newly-created objects.*

#### 5.5.2.6 Explicit: Rules for Management of Security Attributes (FMT_MSA_EXP.1)

**FMT_MSA_EXP.1.1** The TSF shall enforce the following rules for changing security attributes: ***[assignment: for each access right that may be modified, the list of restrictions that exist for each type of user]*.**

*Application Note: For example: To change file security attributes - user must be owner. To change file ownership – user must have capability to take ownership.*

## 5.5.3 Management of TSF Data (FMT_MTD)

### 5.5.3.1 Management of TSF Data (for general TSF data) (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to **create**, change default, query, modify, delete, and clear the **security-relevant TSF data except for audit records, user security attributes, authentication data, and critical security parameters** to **the authorized administrator**.

*Application Note: The restrictions for audit records, user security attributes, authentication data, and critical security parameters are specified below.*

### 5.5.3.2 Management of TSF Data (for audit data) (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to change default, query, delete, and clear the **audit records** to **authorized administrators**.

*Application Note: This selection of "change_default, query, or clear" functions for audit trail management reflect common management functions.*

### 5.5.3.3 Management of TSF Data (for user security attributes) (FMT_MTD.1(3))

FMT_MTD.1.1(3) The TSF shall restrict the ability to **initialize user security attributes** to **authorized administrators**.

### 5.5.3.4 Management of TSF Data (for user security attributes, other than authentication data) (FMT_MTD.1(4))

FMT_MTD.1.1(4) The TSF shall restrict the ability to modify **user security attributes, other than authentication data,** to **authorized administrators.**

### 5.5.3.5 Management of TSF Data (for authentication data) (FMT_MTD.1(5))

FMT_MTD.1.1(5) The TSF shall restrict the ability to modify **authentication data** to **authorized administrators and users authorized to modify their own authentication data.**

### 5.5.3.6 Management of TSF Data (for critical security parameters) (FMT_MTD.1(6))

FMT_MTD.1.1(6) The TSF shall restrict the ability to **initialize and** modify the **critical security parameters** to **cryptographic administrators**.

## 5.5.4 Revocation (FMT_REV)

### 5.5.4.1 Revocation (to authorized administrators) (FMT_REV.1(1))

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to **authorized administrators**.

*Application Note: The term "revoke security attributes" means "change attributes so that access is revoked".*

FMT_REV.1.2(1) The TSF shall enforce the rules:

**a) The revocation of security-relevant authorizations shall be immediate ;**

***b) [Assignment: any other revocation rules concerning access control including the state where access checks are made].***

*Application Note: Security-relevant authorizations include the ability of authorized users to log in or perform privileged operations. An example of revoking a security-relevant authorization is the deletion of a user account upon which system access is immediately terminated).*

#### 5.5.4.2 Revocation (to owners and authorized administrators) (FMT_REV.1(2))

FMT_REV.1.1 (2) **Refinement:** The TSF shall restrict the ability to revoke security attributes **of** objects within the TSC to **owners and authorized administrators**.31

*Application Note: The term "revoke security attributes" means "change attributes so that access is revoked".*

FMT_REV.1.2 (2) The TSF shall enforce the rules:

**a) The revocation of access rights associated with a user, subject, or object shall be enforced when an access check is made;**

**b) *[Assignment: any revocation rules concerning access control including the state attributes where access checks are made].***

*Application Note: The state where access checks are made determines when the access control policy enforces revocation. The access control policy may include immediate or delayed revocation. The access rights are considered to have been revoked when all subsequent access control decisions made by the TSF use the new access control information. In cases where a previous access control decision was made to permit an operation, it is not required that every subsequent operation make an explicit access control decision.*

### 5.5.5 Security Attribute Expiration (FMT_SAE)

#### 5.5.5.1 Time-Limited Authorization (FMT_SAE.1)

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for **security attributes for authorized user authentication data** to **the authorized administrator**.

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to **lock out the associated authorized user account** after the expiration time for the indicated security attribute has passed.

### 5.5.6 Security Management Roles (FMT_SMR)

#### 5.5.6.1 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles:

**a) authorized administrator;**

*Application Note: Any user that is authorized to bypass the MAC, MIC, or DAC policy is, by definition, an authorized administrator. The TOE may provide multiple administrator roles (audit administrator, security administrator, etc).*

**b) cryptographic administrator (i.e., users authorized to perform cryptographic initialization and management functions);**

**c) [assignment: any other roles].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

#### 5.5.6.2 Assuming Roles (FMT_SMR.3)

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles:

**a) authorized administrator;**

**b) cryptographic administrator;**

**c) [assignment: any other roles requiring an explicit request].**

## 5.6 Protection of the TOE Security Functions (FPT)

### 5.6.1 Underlying Abstract Machine Test (FPT_AMT)

#### 5.6.1.1 Abstract Machine Testing (FPT_AMT.1)

FPT_AMT.1.1 **Refinement:** The TSF shall run a suite of tests during the initial start-up, periodically during normal operation, or at the request of an authorized **administrator** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

*Application Note: The test suite need only cover aspects of the underlying abstract machine on which the TSF relies to implement required functions, including domain separation.*

### 5.6.2 Internal TOE TSF Data Transfer (FPT_ITT)

#### 5.6.2.1 Basic Internal TSF Data Transfer Protection (FPT_ITT.1)

FPT_ITT.1.1 **Refinement:** The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE **through the use of encryption**.

#### 5.6.2.2 TSF Data Integrity Monitoring (FPT_ITT.3)

FPT_ITT.3.1 **Refinement:** The TSF shall be able to detect modification and substitution of data for TSF data transmitted between separate parts of the TOE **through the use of cryptographic means**.

*Application Note: Use of a keyed hash function (e.g., HMAC) that is: (1.) calculated over the TSF data to be transmitted, (2.) appended to the transmitted TSF data, and (3.) checked by the receiving part of the TOE is an example of a cryptographic means that detects modification and substitution of such data. Another example is the use of a cryptographic signature over the transmitted TSF data.*

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions:

**a) reject data**

**b) audit event**

**c) [assignment: specify the action to be taken].**

*Application Note: Additional actions ST author might consider are: retransmission of data and, an alarm after reaching a retransmission threshold.*

### 5.6.3 Trusted Recovery (FPT_RCV)

#### 5.6.3.1 Manual Recovery (FPT_RCV.1)

FPT_RCV.1.1 **Refinement:** After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. **As part of the secure state, the cryptographic module shall be in a known and secure state such that all critical areas are empty of plaintext/red/secret data and inaccessible to processes, and all security policies are enforced**.

### 5.6.4 Reference Mediation (FPT_RVM)

#### 5.6.4.1 Non-Bypassability of the TSF (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

### 5.6.5 Domain Separation (FPT_SEP)

#### 5.6.5.1 SFP Domain Separation (FPT_SEP.2)

FPT_SEP.2.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.2.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_SEP.2.3 **Refinement:** The TSF shall maintain the part of the TSF related to **cryptography** in a security domain for **its** own execution that protects it from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to cryptography.**32**

## 5.6.6 Time Stamps (FPT_STM)

### 5.6.6.1 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

*Application Note: A time stamp includes the correct date and time.*

## 5.6.7 Inter-TSF TSF Data Consistency (FPT_TDC)

### 5.6.7.1 Inter-TSF Basic TSF Data Consistency (FPT_TDC.1)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **objects and their security attributes** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *[assignment: list of interpretation rules to be applied by the TSF]* when interpreting the TSF data from another trusted IT product.

## 5.6.8 Internal TOE TSF Data Replication Consistency (FPT_TRC)

### 5.6.8.1 Internal TSF Data Consistency (FPT_TRC.1)

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

*Application Note: Data is interpreted to be consistent and its behavior is also consistent.*

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for **access to objects by users**.

## 5.6.9 TSF Self Testing (FPT_TST)

### 5.6.9.1 TSF Testing (for TSF) (FPT_TST.1(1))

FPT_TST.1.1(1) The TSF shall run a suite of self tests during the initial start-up, periodically during normal operation, **or at the request of an authorized administrator** to demonstrate the correct operation of the TSF.

FPT_TST.1.2(1) **Refinement:** The TSF shall provide authorized **administrators** with the capability to verify the integrity of TSF data.**33**

FPT_TST.1.3(1) **Refinement:** The TSF shall provide authorized **administrators** with the capability to verify the integrity of stored TSF executable code.**34**

### 5.6.9.2 TSF Testing (for cryptography) (FPT_TST.1(2))

FPT_TST.1.1(2) **Refinement:** The TSF shall run a suite of self tests **in accordance with FIPS PUB 140-1, Level 4 (as identified in Table 5.3)** during initial start-up **(on power on)**, at the request of the **cryptographic administrator (on demand), under various conditions,** and periodically **(at least once a day)** to demonstrate the correct operation of the **following:35**

**a) key error detection;**

**b) software/firmware;**

**c) cryptographic algorithms;**

**d) RNG/PRNG; and**

**e) other FIPS PUB 140-1 critical functions;**

**f)** ***[assignment: list of all critical security functions]***.

**Table 5.3 - Interpretation of FIPS PUB 140-1 Self-tests**

| | **FIPS-140 Security Level 4** |
|---|---|
| **Software/Firmware Integrity Tests** | • on power on<br>• on demand<br>• conditional |
| **Cryptographic Algorithm Tests** | • on power on<br>• on demand<br>• conditional |
| **Other FIPS PUB 140-1 critical functions tests and other tests as determined by FIPS PUB 140-1, Appendix A** | • on power on<br>• on demand<br>• conditional |
| **Statistical RNG/PRNG tests** | • on power on<br>• on demand |

FPT_TST.1.2(2) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of **cryptographically related** TSF data.**36**

FPT_TST.1.3(2) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of stored **cryptographically related** TSF executable code.**37**

#### 5.6.9.3 TSF Testing (for key generation components) (FPT_TST.1(3))

FPT_TST.1.1(3) **Refinement**: The TSF shall perform self tests **immediately after generation of a key** to demonstrate correct operation **of each key generation component**. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140 for failing a self-test, and this event will be audited.**38**

*Application Note: Key generation components are those critical elements that compose the entire key generation process (e.g., any algorithms, any RNG/PRNGs, any key generation seeding processes, etc.).*

FPT_TST.1.2(3) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of TSF data **related to the key generation**.**39**

FPT_TST.1.3(3) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the key generation**.**40**

# 5.7 Resource Utilization (FRU)

## 5.7.1 Resource Allocation (FRU_RSA)

#### 5.7.1.1 Maximum Quotas (for disk space and system memory) (FRU_RSA.1(1))

FRU_RSA.1.1(1) The TSF shall enforce maximum quotas of the following resources: **percentage of disk space and percentage of system memory** that individual users can use over a specified period of time.

#### 5.7.1.2 Maximum Quotas (for processing time)(FRU_RSA.1(2))

FRU_RSA.1.1(2) The TSF shall enforce maximum quotas of the following resources: **percentage of processing time** that subjects can use over a specified period of time.

*Application Note: The algorithm to determine percentages of time can be based on many factors (e.g., number of users, relative priority of users, availability of resources to users).*

# 5.8 TOE Access (FTA)

## 5.8.1 Session Locking (FTA_SSL)

#### 5.8.1.1 TSF-Initiated Session Locking (FTA_SSL.1)

FTA_SSL.1.1 **Refinement:** The TSF shall lock an interactive session after *[assignment: a time interval of user inactivity]* by:

a) Clearing or overwriting display devices, making the current contents unreadable.

b) Disabling any activity of the user's data access/display devices other than unlocking the session.

**c) *[Assignment: Other means of locking the interactive]*.**

FTA_SSL.1.2 The TSF shall require the following event to occur prior to unlocking the session:

**a) The TSF shall require the user to re-authenticate prior to unlocking the session (see FIA_AFL_US_INTERP_EXP.1.2 and FTP_TRP.1).**

***b) [Assignment: Other events].***

#### 5.8.1.2 User-Initiated Locking (FTA_SSL.2)

FTA_SSL.2.1 **Refinement:** The TSF shall allow user-initiated locking of the user's own interactive session by:

a) Clearing or overwriting display devices, making the current contents unreadable.

b) Disabling any activity of the user's data access/display devices other than unlocking the session.

**c) *[Assignment: Other means of locking the interactive session]*.**

FTA_SSL.2.2 The TSF shall require the following event to occur prior to unlocking the session:

- **The TSF shall require the user to re-authenticate prior to unlocking the session (see FIA_AFL_US_INTERP_EXP.1.2).**

### 5.8.2 TOE Access Banners (FTA_TAB)

#### 5.8.2.1 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 **Refinement:** Before establishing a user session, the TSF shall display an advisory **notice and consent** warning message regarding unauthorized use of the TOE.

### 5.8.3 TOE Access History (FTA_TAH)

#### 5.8.3.1 TOE Access History (FTA_TAH.1)

FTA_TAH.1.1 **Refinement:** Upon successful session establishment, the TSF shall display the date, time, and location of the last successful session establishment to the **authorized** user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the date, time, and location of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 **Refinement:** The TSF shall not erase the access history information from the **authorized** user interface without giving the user the opportunity to review the information.

# 5.9 Trusted Path/Channels (FTP)

## 5.9.1 Trusted Path (FTP_TRP)

### 5.9.1.1 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

*Application Note: This "distinct" path is merely invoked for the duration of its being needed (e.g., for reauthenticating the user); it need not be invoked for the duration of the user's session.*

FTP_TRP.1.2 The TSF shall permit local users and remote users to initiate communication via the trusted path.

FTP_TRP.1.3 **Refinement:** The TSF shall require the use of the trusted path for user authentication **and user identification**.[41]

# End Notes

This section records the functional requirements where deletion of Common Criteria text were performed.

---

**1** A deletion of CC text was performed in FAU_ARP.1.1. Rationale: The word "take" was deleted for clarity and better flow of the requirement.

FAU_ARP.1.1 **Refinement:** The TSF shall ~~take~~ **generate a warning for the authorized administrator** upon detection of a potential security violation.

**2** A deletion of CC text was performed in FAU_SAR.1.2. Rationale: The word "user" was deleted to replace it with the defined role of "authorized administrator".

FAU_SAR.1.2 **Refinement:** The TSF shall provide the audit records in a manner suitable for the ~~user~~ **authorized administrator** to interpret the information **using a tool to access the audit trail**.

**3** A deletion of CC text was performed in FAU_STG.4.1. Rationale: The words " user with special rights" and "if the audit trail is full " were deleted for clarity and better flow of the requirement. "User with special rights was replace with the authorized administrator role inside the selection. The phrase "if the audit trail is full" was moved to the beginning of the element and changed to say "When the audit trail becomes full". This was done for the element to read more clear since it's the condition that needs to happen in this element.

FAU_STG.4.1 - **Refinement**: When the audit trail becomes full, the TSF shall **provide the authorized administrator the capability to** prevent auditable events , except those taken by the authorized ~~user with special rights~~ **administrator (in the context of performing TOE maintenance)** and **generate an alarm to the authorized administrator**~~, if the audit trail is full~~.

**4** A deletion of CC text was performed in FCS_CKM.1.1(1). Rationale: The words and assignment " and specified cryptographic key sizes [*assignment: cryptographic key sizes*] " were deleted for clarity and better flow of the requirement. The symmetric key generation uses a random number generator that can be implemented in a number of way and using different schemes. By deleting the CC words, the element better states the intended requirement.

FCS_CKM.1.1(1) **Refinement:** The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **as follows**: ***[selection:***

***(1) a hardware random number generator (RNG) as specified in FCS_COP_EXP.2, but with a NIST-approved hashing function (currently SHA-1) required for mixing, and/or***

***(2) a software random number generator (RNG) as specified in FCS_COP_EXP.2, and/or***

***(3) a key establishment scheme based upon public key cryptography using a software random number generator (RNG) as specified in FCS_COP_EXP.2, and/or a hardware random number generator (RNG) as specified in FCS_COP_EXP.2, but with a NIST-approved hashing function (currently SHA-1) required for mixing].***

~~and specified cryptographic key sizes [*assignment: cryptographic key sizes*]~~ that meet the following …

**5** A deletion of CC text was performed in FCS_CKM.1.1(2). Rationale: The words "specified cryptographic key generation algorithm " and " and specified cryptographic key sizes [assignment: *cryptographic key sizes*] " were deleted for clarity and better flow of the requirement. The parameters for generating asymmetric keys can be generated by using different criteria. By deleting the CC words, the element better states the intended requirement.

FCS_CKM.1.1(2) **Refinement:** The TSF shall generate **asymmetric** cryptographic keys in accordance with a ~~specified cryptographic key generation algorithm~~ **domain parameter generator** and ***[selection:***

***(1) a random number generator and/or***

***(2) a prime number generator]***.

~~and specified cryptographic key sizes [*assignment: cryptographic key sizes*]~~ that meet the…

**6** A deletion of CC text was performed in FCS_CKM.4.1. Rationale: The words "specified" and the assignment "[assignment: cryptographic key destruction method]" were deleted for because FIPS PUB 140-1 does not provide specific names for the key destruction method.

FCS_CKM.4.1: **Refinement:** The TSF shall destroy cryptographic keys in accordance with a ~~specified~~ **cryptographic key destruction method** ~~[assignment: *cryptographic key destruction method*]~~ that meets …

**7** A deletion of CC text was performed in FCS_COP.1.1(1). Rationale: The word "specified" was deleted for clarity and better flow of the requirement.

FCS_COP.1.1(1) **Refinement**: The TSF shall perform **data encryption/decryption services** in accordance with a ~~specified~~ **NIST-approved** cryptographic algorithm **Triple Data Encryption Algorithm (TDEA)** and cryptographic key size~~s~~ **of 168 bits (three independent keys)** that meets …

**8** A deletion of CC text was performed in FCS_COP.1.1(2). Rationale: The words "a specified cryptographic" were deleted for clarity and better flow of the requirement

FCS_COP.1.1(2) **Refinement**: The TSF shall perform **cryptographic signature services** in accordance with ~~a specified cryptographic~~ the **NIST-approved digital signature** algorithm ***[selection:***

**(1) Digital Signature Algorithm (DSA) with a key size (modulus) greater than 3000 bits,**

**(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) greater than 3000 bits, or**

**(3) Elliptic Curve Digital Signature Algorithm (ECDSA)]with a key size of 256 bits or greater]**

that meets …

**9** A deletion of CC text was performed in FCS_COP.1.1(3). Rationale: The words "a specified cryptographic" and "cryptographic key sizes " were deleted and replaced with words specific to the required operation for better flow of the requirement.

FCS_COP.1.1(3) **Refinement:** The TSF shall perform **cryptographic hashing services** in accordance with ~~a specified cryptographic~~ **the NIST-approved hash** algorithm **Secure Hash Algorithm 1 (SHA-1)** and ~~cryptographic key sizes~~ **hash size of 160-bit message digest** that meets the following**: FIPS PUB 180-1**

**10** A deletion of CC text was performed in FCS_COP.1.1(4). Rationale: The words "a specified cryptographic" and "and cryptographic key sizes " were deleted for clarity and better flow of the requirement. The assignment was replaced with a selection that incorporates the algorithm and the key size for the corresponding algorithm.

FCS_COP.1.1(4) **Refinement:** The TSF shall perform **cryptographic key exchange services** in accordance with ~~a specified cryptographic~~ **the NIST-approved key exchange** algorithm ***[selection:***

1. ***Diffie-Hellman Algorithm and cryptographic key sizes greater than 3000 bits,***
2. ***RSA Algorithm and cryptographic key size greater than 3000 bits, or***
3. ***Elliptic Curve Key Exchange Algorithm (ECKEA) and cryptographic key sizes of 256 bits or greater]***

~~and cryptographic key sizes~~ that meet …

**11** A deletion of CC text was performed in FDP_ACC.2.1. Rationale: The words " subjects and objects covered by the SFP" were deleted to for better clarity and flow on the element.

FDP_ACC.2.1 **Refinement:** The TSF shall enforce the **Discretionary Access Control policy** *on [assignment: list of all subjects and* ***all named*** *objects]* and all operations among ~~subjects and objects covered by the SFP~~ **them**.

**12** A deletion of CC text was performed in FDP_ACC.2.2. Rationale: The words "within the TSC" and "an access control SFP" were deleted because there is no need to specify that subjects and objects are within the TSC and to explicitly state the access control policy we are referring to (DAC).

FDP_ACC.2.2 **Refinement:** The TSF shall ensure that all operations between any subject ~~within the TSC~~ and any **named** object are covered by ~~an access control SFP~~ **the Discretionary Access Control policy**.

**13** A deletion of CC text was performed in FDP_ACF_US_INTERP_EXP.1.2. Rationale: The word "controlled" was deleted because there is no need to specify that subjects and objects are controlled.

FDP_ACF_US_INTERP_EXP.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among ~~controlled~~ subjects and ~~controlled~~ named objects is …

**14** A deletion of CC text was performed in FDP_IFC.2.1(1). Rationale: The words "to and from the subjects covered by the SFP" were deleted and substituted with "among them" because it covers all subjects and all objects.

FDP_IFC.2.1(1) **Refinement:** The TSF shall enforce the **Mandatory Access Control policy** on ***[assignment: list of all subjects and all objects]***, and all operations that cause information to flow ~~to and from the subjects covered by the SFP~~ **among them**.

**15** A deletion of CC text was performed in FDP_IFC.2.2(1). Rationale: The words "to and from any subject" were deleted and substituted with "among subjects and objects" because the previous did not cover objects.

FDP_IFC.2.2(1) **Refinement:** The TSF shall ensure that all operations that cause any information in the TSC to flow ~~to and from any subject~~ **among subjects and objects** in the TSC are covered by **the MAC** SFP.

**16** A deletion of CC text was performed in FDP_IFC.2.1(2). Rationale: The words "to and from the subjects covered by the SFP" were deleted and substituted with "among them" because it covers all subjects and all objects.

FDP_IFC.2.1(2) **Refinement:** The TSF shall enforce the **Mandatory Integrity Control policy** on ***[assignment: list of all subjects and all objects]***, and all operations that cause information to flow ~~to and from the subjects covered by the SFP~~ **among them**.

**17** A deletion of CC text was performed in FDP_IFC.2.2(2). Rationale: The words "to and from any subject" were deleted and substituted with "among subjects and objects" because the previous did not cover objects.

FDP_IFC.2.2(2) **Refinement:** The TSF shall ensure that all operations that cause any information in the TSC to flow ~~to and from any subject~~ **among subjects and objects** in the TSC are covered by **the MIC** SFP.

**18** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.1(1). Rationale: The word "information" was deleted because security attributes is defined in the Glossary of Terms as needed in this requirement and not "information security attributes".

FDP_IFF_US_INTERP_EXP.2.1(1) **Refinement:** The TSF shall enforce the **Mandatory Access Control policy** based on the following types of subjects, **objects**, and ~~information~~ security attributes:

**a) [Assignment: list of all subjects]**

**b) the sensitivity label of …**

**19** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.2(1). Rationale: The words "between a controlled subject and controlled information via a controlled operation if" and "based on the ordering relationships between security attributes hold" was deleted because the information flow for this requirement is among subjects and objects.

FDP_IFF_US_INTERP_EXP.2.2(1) **Refinement:** The TSF shall permit an information flow **among subjects and objects** based on the following rules:

**a) If the sensitivity label of …**

**20** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.3(1) Rationale: The words "enforce the" were deleted because it reads better based on the inserted assignment.

FDP_IFF_US_INTERP_EXP.2.3(1) **Refinement:** The TSF shall **provide authorized administrators with a MAC-exempt capability by *[assignment: list of means of invoking MAC-exempt rules]***

**21** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.7(1) Rationale: The words "information flow control" were deleted to be more specific by replacing them with actual MAC information flow control.

FDP_IFF_US_INTERP_EXP.2.7(1) **Refinement:** The TSF shall enforce the following relationships for any two valid information flow control **MAC** security attributes:

**22** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.1(2). Rationale: The word "information" was deleted because security attributes is defined in the Glossary of Terms as needed in this requirement and not "information security attributes".

FDP_IFF_US_INTERP_EXP.2.1(2) **Refinement:** The TSF shall enforce the **Mandatory Integrity Control policy** based on the following types of subjects, **objects**, and ~~information~~ security attributes:

***a) [Assignment: list of all subjects]***

**b) the integrity label of …**

**23** A deletion of CC text was performed in FDP_IFF.2.2(2). Rationale: The words "between a controlled subject and controlled information via a controlled operation if" and "based on the ordering relationships between security attributes hold" was deleted because the information flow for this requirement is among subjects and objects.

FDP_IFF.2.2(2) **Refinement:** The TSF shall permit an information flow **among subjects and objects** based on the following rules:

**a) If the integrity label of …**

**24** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.3(2) Rationale: The words "enforce the" were deleted because it reads better based on the inserted assignment.

FDP_IFF_US_INTERP_EXP.2.3(2) **Refinement:** The TSF shall **provide authorized administrators with a MIC-exempt capability by *[assignment: list of means of invoking MIC-exempt rules].***

**25** A deletion of CC text was performed in FDP_IFF_US_INTERP_EXP.2.7(2) Rationale: The words "information flow control" were deleted to be more specific by replacing them with actual MIC information flow control.

FDP_IFF_US_INTERP_EXP.2.7(2) **Refinement:** The TSF shall enforce the following relationships for any two valid information flow control **MIC** security attributes:

**26** A deletion of CC text was performed in FDP_IFF.3.1. Rational: The words " to limit the capacity of" and " to a [assignment: *maximum capacity*]" were deleted because the authors did not want any illicit information flows to exist and not require AVA_CCA.3. FDP_IFF.5 allows for no illicit information flows but has AVA_CCA.3 as dependency.

FDP_IFF.3.1 **Refinement:** The TSF shall enforce the **Mandatory Access Control policy** ~~to limit the capacity of~~ **ensure that no illicit information flows exist which cross the cryptographic boundaries** ~~to a [assignment: maximum capacity]~~.

**27** A deletion of CC text was performed in FDP_ITC.2.3. Rationale: The words "security attributes" were deleted to replace it for the specific security attribute "validated label".

FDP_ITC.2.3 **Refinement:** The TSF shall ensure that the protocol used provides for the **correct** unambiguous association between the ~~security attributes~~ **validated label** and the user data received.

**28** A deletion of CC text was performed in FMT_MSA.1.1. Rationale: The words " [assignment: list of security attributes]" was deleted for clarity and better flow of the requirement. The value of the object security attributes was already specified in the element before the assignment appeared.

FMT_MSA.1.1 **Refinement:** The TSF shall enforce the Discretionary Access Control policy to restrict the ability to query **and change** the **value of the object** security attributes ~~[assignment: list of security attributes]~~ to **authorized administrators and owners of the object**.

**29** A deletion of CC text was performed in FMT_MSA.1.1(2). Rational: The words "security attributes" were deleted to replace it for the specific security attribute "value of the sensitivity label associated with an object".

FMT_MSA.1.1(2) The TSF shall enforce the **Mandatory Access Control policy** to restrict the ability to **change** the ~~security attributes~~ **value of the sensitivity label associated with an object** to **authorized administrators.**

**30** A deletion of CC text was performed in FMT_MSA.1.1(3). Rational: The words "security attributes" were deleted to replace it for the specific security attribute "value of the integrity label associated with an object "

FMT_MSA.1.1(3) The TSF shall enforce the **Mandatory Integrity Control policy** to restrict the ability to **change** the ~~security attributes~~ **value of the integrity label associated with an object** to **authorized administrators.**

**31** A deletion of CC text was performed in FMT_REV.1.1 (2). Rationale: The words "associated with" were deleted for clarity and better flow of the requirement.

FMT_REV.1.1 (2) **Refinement:** The TSF shall restrict the ability to revoke security attributes ~~associated~~ **of** objects within the TSC to **owners and authorized administrators.**

**32** A deletion of CC text was performed in FPT_SEP.2.3. Rationale: The words "their", "them", and "those SPFs" were deleted for grammatical reasons since this element refers to cryptography and not SPFs.

FPT_SEP.2.3 **Refinement:** The TSF shall maintain the part of the TSF related to **cryptography** in a security domain for ~~their~~ **its** own execution that protects ~~them~~ **it** from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to ~~those SPFs~~ **cryptography**.

**33** A deletion of CC text was performed in FPT_TST.1.2(1). Rationale: The word "users" was deleted to replace it with the role of "authorized administrator". Only authorized administrators should be given the capability to verify the integrity of the TSF data.

FPT_TST.1.2(1) **Refinement:** The TSF shall provide authorized ~~users~~ **administrators** with the capability to verify the integrity of TSF data.

**34** A deletion of CC text was performed in FPT_TST.1.3(1). Rationale: The word " users " was deleted to replace it with the role of "authorized administrator".

FPT_TST.1.3(1) **Refinement:** The TSF shall provide authorized ~~users~~ **administrators** with the capability to verify the integrity of stored TSF executable code.

**35** A deletion of CC text was performed in FPT_TST.1.1(2). Rationale: The word "TSF" was deleted to allow for the demonstration of the correct operation of a number of cryptographic related self test.

FPT_TST.1.1(2) **Refinement:** The TSF shall run a suite of self-**tests in accordance with FIPS PUB 140-1, Level 4 (as identified in Table 5.3)** during initial start-up **(on power on)**, at the request of the **cryptographic administrator (on demand), under various conditions,** and periodically **(at least once a day)** to demonstrate the correct operation of the ~~TSF~~ **following …**

**36** A deletion of CC text was performed in FPT_TST.1.2(2). Rationale: The word "users" was deleted to replace it with the role of " cryptographic administrator". "Only authorized cryptographic administrators should be given the capability to verify the integrity of cryptographically related TSF data.

FPT_TST.1.2 (2) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of **cryptographically related** TSF data.

**37** A deletion of CC text was performed in FPT_TST.1.3(2). Rationale: The word “users” was deleted to replace it with the role of " cryptographic administrator". Only authorized cryptographic administrators should be given the capability to verify the integrity of cryptographically related TSF executable code.

FPT_TST.1.3(2) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of stored **cryptographically related** TSF executable code.

**38** A deletion of CC text was performed in FPT_TST.1.1(3). Rationale: The word "the TSF" was deleted to allow for the demonstration of the correct operation of each key generation component.

FPT_TST.1.1(3) **Refinement:** The TSF shall run a suite of self-tests **immediately after generation of a key** to demonstrate the correct operation of ~~the TSF~~ **each key generation component**. **If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140 for failing a self-test, and this event will be audited.**

**39** A deletion of CC text was performed in FPT_TST.1.2(3). Rationale: The word "users" was deleted to replace it with the role of "cryptographic administrator".

FPT_TST.1.2(3) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of TSF data **related to the key generation**.

**40** A deletion of CC text was performed in FPT_TST.1.3(3). Rationale: The word “users” was deleted to replace it with the role of "cryptographic administrator".

FPT_TST.1.3(3) **Refinement:** The TSF shall provide authorized ~~users~~ **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the key generation**.

**41** A deletion of CC text was performed in FTP_TRP.1.3. Rationale: The word " initial " was deleted from the selection option to increase the scope of the trusted path requirement to include any re-authentication.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ~~initial~~ user authentication **and user identification**.

# 6. Security Assurance Requirements

50 This section contains the detailed security assurance requirements for operating systems supporting multilevel systems in environments requiring medium robustness. The requirements contained in this section are either selected from Part 3 of the CC or have been explicitly stated (with short names ending in "_EXP"). Table 6.1 lists the explicitly stated assurance components.

**Table 6.1 - Explicit Assurance Requirements**

| Explicit Component | Component Behavior Name |
|---|---|
| AVA_CCA_EXP.1 | Cryptographic Module Covert Channel Analysis |

51 The combination of assurance components chosen result in an Evaluated Assurance Level 4 Augmented (EAL4+). The intended TOE environment and the value of information processed by this environment establish the need for the TOE to be evaluated at this EAL level[26]. The augmented assurances required are in the areas of vulnerability analysis/penetration testing, development, and covert channel analysis for cryptography. These security assurance requirements are summarized in Table 6.2.

[26] Refer to the "Mutual Recognition of Common Criteria Certificates" section 1.3 to read conditions for the CC certificate to be mutually recognized for PPs with EALs higher than 4.

**Table 6.2 - Summary of Assurance Components by Evaluation Assurance Level**

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | **EAL4** | EAL5 | EAL6 | EAL7 |
| Configuration Management | ACM_AUT | | | | **1** | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | **4** | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | **2** | 3 | 3 | 3 |
| Delivery and Operation | ADO_DEL | | 1 | 1 | **2** | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | **1** | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | **2** | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | **2** | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | **2** | 3 | 3 |
| | ADV_INT | | | | | **1** | 2 | 3 |
| | ADV_LLD | | | | **1** | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | **1** | 2 | 2 | 3 |
| | ADV_SPM | | | | **1** | 3 | 3 | 3 |
| Guidance Documents | AGD_ADM | 1 | 1 | 1 | **1** | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | **1** | 1 | 1 | 1 |
| Life cycle Support | ALC_DVS | | | 1 | **1** | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | **1** | 2 | 2 | 3 |
| | ALC_TAT | | | | **1** | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | **2** | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | **2** | 2 | 3 |
| | ATE_FUN | | 1 | 1 | **1** | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | **2** | 2 | 2 | 3 |
| Vulnerability Assessment | **AVA_CCA_EXP** | | | | | **1** | **2** | 2 |
| | AVA_MSU | | | 1 | **2** | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | **1** | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | **3** | 4 | 4 |

# 6.1 Configuration Management (ACM)

## 6.1.1 CM Automation (ACM_AUT)

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.1.2 CM Capabilities (ACM_CAP)

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.1.3 CM Scope (ACM_SCP)

ACM_SCP.2.1D The developer shall provide CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## 6.2 Delivery and Operation (ADO)

### 6.2.1 Delivery (ADO_DEL)

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.2.2 Installation, Generation and Start-up (ADO_IGS)

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

## 6.3 Development Documentation (ADV)

### 6.3.1 Functional Specification (ADV_FSP)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

### 6.3.2 High-Level Design (ADV_HLD)

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C **Refinement:** The high-level design shall describe the security functionality provided by each subsystem of the TSF **including the cryptographic subsystem**.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C **Refinement:** The high-level design shall identify all interfaces to the subsystems of the TSF **including the cryptographic subsystem**.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 6.3.3 Implementation Representation (ADV_IMP)

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

ADV_IMP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

### 6.3.4 TSF Internals (ADV_INT)

ADV_INT.1.1D **Refinement:** The developer shall design and structure the TSF in a modular fashion **including a cryptographic module separate from other processes** that avoids unnecessary interactions between the modules of the design.

ADV_INT.1.2D The developer shall provide an architectural description.

ADV_INT.1.1C The architectural description shall identify the modules of the TSF.

*Application Note: The cryptographic module is part of the TSF.*

ADV_INT.1.2C The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

ADV_INT.1.3C The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

ADV_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_INT.1.2E The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

### 6.3.5 Low-level Design (ADV_LLD)

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C **Refinement:** The low-level design shall describe how each TSP-enforcing function is provided **and describe the state-transitions of the cryptographic module**.

ADV_LLD.1.7C **Refinement:** The low-level design shall identify all interfaces to the modules of the TSF **including the physical/logical ports of the cryptographic module**.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 6.3.6 Representation Correspondence (ADV_RCR)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.3.7 Security Policy Modeling (ADV_SPM)

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

*Application Note: Security policies that can be modeled include descriptions of at least the following security policies: Identification and Authentication, Discretionary Access Control, Mandatory Access Control, Control, Mandatory Integrity, Audit, and Cryptography.*

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

# 6.4 Guidance Documents (AGD)

## 6.4.1 Administrator Guidance (AGD_ADM)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

*Application Note: Administrators of the TOE include the "authorized administrator" and "cryptographic administrator" roles (see FMT_SMR.1).*

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.4.2 User Guidance (AGD_USR)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

*Application Note: This includes guidance for the users of the cryptographic module.*

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## 6.5 Life Cycle Support (ALC)

### 6.5.1 Development Security (ALC_DVS)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

### 6.5.2 Flaw Remediation (ALC_FLR)

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.5.3 Life Cycle Definition (ALC_LCD)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.5.4 Tools and Techniques (ALC_TAT)

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1C All development tools used for implementation shall be well defined.

*Application Note: The development tools include the compiler used to generate the TOE.*

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

*Application Note: This documentation includes the compiler options used during the generation of the TOE.*

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## 6.6 Testing (ATE)

### 6.6.1 Coverage (ATE_COV)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.6.2 Depth (ATE_DPT)

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.6.3 Functional Tests (ATE_FUN)

ATE_FUN.1.1D **Refinement:** The developer shall test the TSF **including stress testing the boundary conditions of all interfaces** and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 6.6.4 Independent Testing (ATE_IND)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

# 6.7 Vulnerability Assessment (AVA)

## 6.7.1 Explicit: Cryptographic Module Covert Channel Analysis (AVA_CCA_EXP)

*Application Note: The covert channel analysis is performed only upon the cryptographic module; a search is made for the leakage of critical security parameters, rather than a violation of an information control policy.*

**AVA_CCA_EXP.2.1D For the cryptographic module,** the developer shall conduct a search for covert channels for the **leakage of critical security parameters**.

*Application Note: The remainder of the TOE need not be subjected to a covert channel analysis.*

**AVA_CCA_EXP.2.2D** The developer shall provide covert channel analysis documentation.

**AVA_CCA_EXP.2.1C** The analysis documentation shall identify covert channels **in the cryptographic module** and estimate their capacity.

**AVA_CCA_EXP.2.2C** The analysis documentation shall describe the procedures used for determining the existence of covert channels **in the cryptographic module**, and the information needed to carry out the covert channel analysis.

**AVA_CCA_EXP.2.3C** The analysis documentation shall describe all assumptions made during the covert channel analysis.

**AVA_CCA_EXP.2.4C** The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

**AVA_CCA_EXP.2.5C** The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

**AVA_CCA_EXP.2.6C** The analysis documentation shall provide evidence that the method used to identify covert channels is systematic.

**AVA_CCA_EXP.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AVA_CCA_EXP.2.2E** The evaluator shall confirm that the results of the covert channel analysis show that the **cryptographic module** meets its functional requirements.

**AVA_CCA_EXP.2.3E Refinement:** The evaluator shall selectively validate the covert channel analysis through **independent analysis and** testing.

### 6.7.2 Misuse (AVA_MSU)

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

### 6.7.3 Strength of TOE security functions (AVA_SOF)

*Application Note: The security functions, for which strength of function claims are made, are identified in sections 5.4.3.*

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

### 6.7.4 Vulnerability Analysis (AVA_VLA)

AVA_VLA.3.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.3.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.3.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.3.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

# 7. Rationale

52 This section provides the rationale for the selection, creation, and use of security objectives and requirements.

## 7.1 Security Objectives derived from Threats

53 Each of the identified threats to security is addressed by one or more security objectives. The table below summarizes this mapping; this is then followed by explanatory text of how this mapping was derived for each threat.

**Table 7.1 – Mapping of Security Objectives to Threats**

| Threat | Addressing Assumptions / Resultant Objectives |
|---|---|
| T.ADMIN_ERROR | O.ADMIN_ROLE<br>O.ADMIN_TRAINED<br>O.MANAGE |
| T.ADMIN_ROGUE | O.ADMIN_ROLE |
| T.AUDIT_CORRUPT | OE.PHYSICAL<br>O.ACCESS<br>O.ADMIN_TRAINED<br>O.AUDIT_PROTECTION<br>O.MANAGE<br>O.SELF_PROTECTION |
| T.CONFIG_CORRUPT | OE.PHYSICAL<br>O.ACCESS<br>O.ADMIN_TRAINED<br>O.MANAGE<br>O.SELF_PROTECTION |
| T.DATA_NOT_SEPARATED | O.ACCESS<br>O.MANDATORY_ACCESS<br>O.MANDATORY_INTEGRITY<br>O.MARKINGS<br>O.RESIDUAL_INFORMATION |
| T.DOS | O.RESOURCE_SHARING |

| | |
|---|---|
| T.EAVESDROP | O.ENCRYPTED_CHANNEL<br>O.ENCRYPTION_SERVICES<br>O.PROTECT<br>O.SELF_PROTECTION |
| T.INSECURE_START | O.ADMIN_TRAINED<br>O.MANAGE<br>O.RECOVERY<br>O.TRUSTED_SYSTEM_OPERATION |
| T.IMPROPER_INSTALLATION | O.ADMIN_TRAINED<br>O.INSTALL<br>O.MANAGE |
| T.MASQUERADE | O.ENCRYPTED_CHANNEL<br>O.TRUSTED_PATH<br>O.TSF_CRYPTOGRAPHIC_INTEGRITY<br>O.USER_AUTHENTICATION<br>O.USER_IDENTIFICATION |
| T.OBJECTS_NOT_CLEAN | O.RESIDUAL_INFORMATION |
| T.POOR_DESIGN | O.CONFIG_MGMT<br>O.SOUND_DESIGN<br>O.VULNERABILITY_ANALYSIS |
| T.POOR_IMPLEMENTATION | O.PENETRATION_TEST<br>O.SOUND_IMPLEMENTATION<br>O.TESTING<br>O.VULNERABILITY_ANALYSIS |
| T.POOR_TEST | O.PENETRATION_TEST<br>O.TRUSTED_SYSTEM_OPERATION<br>O.TESTING |
| T.REPLAY | O.ACCESS_HISTORY<br>O.ENCRYPTED_CHANNEL<br>O.ENCRYPTION_SERVICES<br>O.TSF_CRYPTOGRAPHIC_INTEGRITY |

| | |
|---|---|
| T.SPOOFING | O.ENCRYPTED_CHANNEL<br>O.ENCRYPTION_SERVICES<br>O.TSF_CRYPTOGRAPHIC_INTEGRITY<br>O.TRUSTED_PATH |
| T.SYSACC | OE.PHYSICAL<br>O.ACCESS<br>O.ACCESS_HISTORY<br>O.ADMIN_TRAINED<br>O.MANAGE<br>O.USER_AUTHENTICATION<br>O.USER_IDENTIFICATION |
| T.UNATTENDED_SESSION | O.ACCESS<br>O.PROTECT<br>O.TRAINED_USERS<br>O.USER_AUTHENTICATION |
| T.UNAUTH_ACCESS | OE.PHYSICAL<br>O.ACCESS<br>O.DISCRETIONARY_ACCESS<br>O.MANDATORY_ACCESS<br>O.MANDATORY_INTEGRITY<br>O.PROTECT<br>O.SELF_PROTECTION |
| T.UNAUTH_MODIFICATION | OE.PHYSICAL<br>O.ACCESS<br>O.DISCRETIONARY_ACCESS<br>O.MANDATORY_ACCESS<br>O.MANDATORY_INTEGRITY<br>O.SELF_PROTECTION |
| T.UNDECTED_ACTIONS | OE.PHYSICAL<br>O.AUDIT_GENERATION<br>O.ACCESS_HISTORY<br>O.AUDIT_PROTECTION |

| | |
|---|---|
| T.UNIDENTIFIED_ACTIONS | O.AUDIT_REVIEW<br>O.MANAGE<br>O.ADMIN_TRAINED |
| T.UNKNOWN_STATE | O.RECOVERY |
| T.USER_CORRUPT | O.ACCESS<br>O.DISCRETIONARY_ACCESS<br>O.DISCRETIONARY_USER_CONTROL<br>O.MANDATORY_ACCESS<br>O.MANDATORY_INTEGRITY<br>O.PROTECT |

**T.ADMIN_ERROR** - *Improper administration may result in defeat of specific security features.*

Improper administration could result if the administrator is incompetent, unknowledgeable, or untrustworthy. Administrative roles isolate the amount of damage an authorized administrator can perform (O.ADMIN_ROLE). So long as the TOE provides the necessary administrator support (O.MANAGE) and the administrator is properly trained (O.ADMIN_TRAINED), this threat should be eliminated.

**T.ADMIN_ROGUE –** *Authorized administrator's intentions may become malicious resulting in TSF data to be compromised.*

Authorized administrators intentions may become malicious. Administrative roles isolate the amount of damage an authorized administrator can perform (O.ADMIN_ROLE).

**T.AUDIT_CORRUPT** - *A malicious process or user may cause audit records to be lost or modified, or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.*

Tampering or destruction of audit data by physical means is addressed by the environment (OE.PHYSICAL). Destroying or corrupting audit data by other means necessitates an objective that the IT system controls access to its resources (O.ACCESS). Because audit data is considered to be TSF data, there is an objective for the TSF to protect itself (O.SELF_PROTECTION) and its data (O.AUDIT_PROTECTION). Administrators may lose or destroy audit data if they are not trained (O.ADMIN_TRAINED) in the use of the administrative facilities available to them (O.MANAGE).

**T.CONFIG_CORRUPT** - *A malicious process or user may cause configuration data or other trusted data to be lost or modified.*

Tampering or destruction of configuration data by physical means is addressed by the environment (OE.PHYSICAL). Destroying or corrupting configuration data by other means necessitates an objective that the IT system controls access to its resources (O.ACCESS). Because configuration data is considered to be TSF data, there is an objective for the TSF to protect itself (O.SELF_PROTECTION) and its data. Administrators may lose or destroy configuration data if they are not trained (O.ADMIN_TRAINED) in the use of the administrative facilities available to them (O.MANAGE).

**T.DATA_NOT_SEPARATED -** *Systems may not adequately separate the data on the basis of its label, thereby allowing people improper access to labeled data.*

Addressing this threat requires that data be labeled appropriately (O.MARKINGS) and that an access control policy (O.MANDATORY_ACCESS) and integrity policy (O.MANDATORY_INTEGRITY) based upon those labels be enforced. There is also an objective to prohibit users from accessing inappropriately labeled data that had been stored in system resources previously allocated to other users (O.RESIDUAL_INFORMATION). The IT system can thereby control access to the resources it controls (O.ACCESS).

**T.DOS -** *A malicious process or user may block others from system resources via a resource exhaustion denial of service attack.*

Addressing this threat produces an objective of ensuring that no user can block others from accessing its resources (O.RESOURCE_SHARING).

**T.EAVESDROP -** *A malicious process or user may intercept transmitted data inside or outside of the enclave.*

This threat is addressed encrypting the communication line (O.ENCRYPTED_CHANNEL), thereby protecting any TSF data (O.SELF_PROTECTION) or user data (O.PROTECT) from being observed by users who are not authorized to see them (O.ENCRYPTION_SERVICES).

**T.IMPROPER_INSTALLATION -** *Operating system may be delivered , installed, or configured in a manner that undermines security.*

Trusted personnel might start the system up in an unsecure state (O.INSTALL) if they are not trained (O.ADMIN_TRAINED) in the use of the administrative facilities available to them (O.MANAGE).

**T.INSECURE_START -** *Reboot may result in insecure state of the operating system.*

Addressing this threat produces the objective of bringing up the system in a secure state (O.RECOVERY), thereby maintaining security (O.TRUSTED_SYSTEM_OPERATION). Administrators might start the system up in an unsecure state if they are not trained

(O.ADMIN_TRAINED) in the use of the administrative facilities available to them (O.MANAGE).

**T.MASQUERADE -** *A malicious process or user on one machine on the network may masquerade as an entity on another machine on the same network.*

Addressing the threat of a malicious process masquerading as the TSF produces an objective of providing users with a means of ensuring they are really communicating with the TSF (O.TRUSTED_PATH). Addressing the threat of a user masquerading as a different user produces an objective of identifying the users (O.USER_IDENTIFICATION) reliably (O.USER_AUTHENTICATION). The threat of masquerading by use of session hijacking is addressed by protecting the communications channel against disclosure (O.ENCRYPTED_CHANNEL) and modification (O.TSF_CRYPTOGRAPHIC_INTEGRITY).

**T.OBJECTS_NOT_CLEAN** - *Systems may not adequately remove the data from objects between usage by different users, thereby releasing information to a user unauthorized for the data.*

Addressing this threat prohibits users from accessing data that had been stored in system resources previously allocated to other users (O.RESIDUAL_INFORMATION).

**T.POOR_DESIGN** - *Unintentional or intentional errors in requirement specification, design or development of the IT operating system may occur.*

Faults in the TOE's design can be reduced by eliminating errors in logic (O.SOUND_DESIGN) and by carefully tracking the changes being made (O.CONFIG_MGMT). The introduction of faults in the design can be reduced by looking for vulnerabilities that might be introduced (O.VULNERABILITY_ANALYSIS). Poor designs that are correctly implemented can be uncovered by testing (O.TESTING and O.PENETRATION_TEST).

**T.POOR_IMPLEMENTATION -** *Unintentional or intentional errors in implementing the design of the IT operating system may occur.*

Faults in the TOE's implementation can be reduced by validating (O.TESTING) that it is a faithful instantiation of its design (O.SOUND_ IMPLEMENTATION). Additionally, faults in implementation can be reduced by looking for vulnerabilities that might have been introduced (O.VULNERABILITY_ANALYSIS) and by testing to see if such vulnerabilities exist (O.PENETRATION_TEST). Introduction of errors can also be reduced by the tracking of changes (O.CONFIG_MGMT)

**T.POOR_TEST -** *Incorrect system behavior may result from inability to demonstrate that all functions and interactions within the operating system operation are correct.*

This threat deals with the inability to tell whether the tests (O.TESTING) are sufficient to show that the TOE is maintaining its security (O.TRUSTED_SYSTEM_OPERATION). Addressing this threat will show adequate testing (O.PENETRATION_TEST).

**T.REPLAY -** *A malicious process or user may gain access by replaying authentication (or other) information.*

Replaying authentication information would allow the wrong person to access the resources protected by the TOE. Users can be alerted to the fact that someone has replayed their authentication information if the TOE informs them at each login of the previous login (O.ACCESS_HISTORY). Some types of encryption (O.ENCRYPTED_CHANNEL, O.ENCRYPTION_SERVICES), such as a different key per session can reduce the possibility of replay attacks. Timestamp accesses may replayed unless there is a means to protect the integrity of the timestamp (O.TSF_CRYPTOGRAPHIC_INTEGRITY).

**T.SPOOFING -** *A hostile entity may masquerade itself as the IT operating system and communicate with authorized users who incorrectly believe they are communicating with the IT operating system.*

Addressing this threat produces an objective of providing users with a means of ensuring they are really communicating with the TSF (O.TRUSTED_PATH). Spoofing can also be obviated through digital signature means (O.ENCRYPTION_SERVICES, O.TSF_CRYPTOGRAPHIC_INTEGRITY). Spoofing aimed at obtaining cryptanalytic advantage can be prevented by hiding message content (O.ENCRYPTED_CHANNEL).

**T.SYSACC -** *A malicious process or user may gain unauthorized access to the administrator account, or that of other trusted personnel.*

The threat of the wrong individual accessing the administrator's account (O.ACCESS) may be addressed by physical means (OE.PHYSICAL), such as in cases where the administrator console is behind a locked door. For other cases, accessing the administrator account may be achieved after being identified (O.USER_IDENTIFICATION) and authenticated (O.USER_AUTHENTICATION). Administrators can be alerted to the fact that someone had logged into their account using the correct authentication data if the TOE informs them at each login of the previous login (O.ACCESS_HISTORY); the administrator will have to know (O.ADMIN_TRAINED) to check this information (O.MANAGE) at each login.

**T.UNATTENDED_SESSION** - *A malicious process or user may gain unauthorized access to an unattended session*

Unattended sessions must be protected (O.PROTECT) from unauthorized access (O.ACCESS). This might be accomplished by simply alerting users that they must not leave sessions unattended (O.TRAINED_USERS) or by requiring users to reauthenticate themselves (O.USER_AUTHENTICATION) after returning to the unattended session.

**T.UNAUTH_ACCESS -** *Unauthorized access to data by a user may occur.*

The threat of unauthorized physical access is addressed by the environment (OE.PHYSICAL). Addressing the threat of other unauthorized access results in objectives of either protecting the user data (O.PROTECT) or TSF data or resources (O.SELF_PROTECTION) from unauthorized access (O.ACCESS). Access to user data may be either discretionary (O.DISCRETIONARY_ACCESS) or mandatory (O.MANDATORY_ACCESS) disclosure access, or mandatory (O.MANDATORY_INTEGRITY) integrity access.

**T.UNAUTH_MODIFICATION -** *Unauthorized modification or use of IT operating system attributes and resources may occur.*

The threat of unauthorized modification of system attributes or resources resulting from physical access is addressed by the environment (OE.PHYSICAL). Addressing the threat of other unauthorized modification results in objectives of protecting TSF data or resources (O.SELF_PROTECTION) from unauthorized modification (O.ACCESS). Access to user data may be either discretionary (O.DISCRETIONARY_ACCESS) or mandatory (O.MANDATORY_ACCESS) disclosure access, or mandatory (O.MANDATORY_INTEGRITY) integrity access.

**T.UNDETECTED_ACTIONS -** *Failure of the IT operating system to detect and record unauthorized actions may occur.*

The threat of undetected physical manipulation of the TOE is addressed by the physical protection provided by the environment (OE.PHYSICAL). Other actions are detected and a record is made (O.AUDIT_GENERATION). To prevent removing evidence, the audit records need to be protected (O.AUDIT_PROTECTION). And to detect another user having compromised an account by replaying the authentication information, there needs to be information related the previous login (O.ACCESS_HISTORY).

**T.UNIDENTIFIED_ACTIONS -** *Failure of the administrator to identify and act upon unauthorized actions may occur.*

The threat of an administrator failing to know about audit events produces the objectives of the administrator having the facilities (O.MANAGE) to review audit records (O.AUDIT_REVIEW) and knowing how to do so (O.ADMIN_TRAINED).

**T.UNKNOWN_STATE -** *Upon failure of the IT operating system, the security of the IT operating system may be unknown.*

Addressing this threat produces the objective of the system coming up in a secure state (O.RECOVERY).

**T.USER_CORRUPT -** *User data may be lost or tampered with by other users.*

This threat requires protecting user data (O.PROTECT) from unauthorized access (O.ACCESS). Authorized access may be either according to a discretionary (O.DISCRETIONARY_ACCESS) or mandatory (O.MANDATORY_ACCESS) access policy, or by a mandatory integrity policy (O.MANDATORY_INTEGRITY). The discretionary access control policy is enforced based upon attributes set by the owners of the objects (O.DISCRETIONARY_USER_CONTROL).

## 7.2 Objectives derived from Security Policies

54 Each of the identified security policies implies a set of security objectives to be met. The table below summarizes this mapping; this is then followed by explanatory text of how this mapping was derived for each policy.

**Table 7.2 – Mapping of Security Objectives to Security Policies**

| Policies | Objectives enforcing Policies |
|---|---|
| P.ACCESS_BANNER | O.DISPLAY_BANNER |
| P.ACCOUNT | O.AUDIT_GENERATION<br>O.AUDIT_REVIEW<br>O.USER_IDENTIFICATION |
| P.AUTHORIZATION | O.ACCESS<br>O.PROTECT<br>O.USER_IDENTIFICATION |
| P.AUTHORIZED_USERS | O.USER_AUTHENTICATION<br>O.USER_IDENTIFICATION |
| P.CLEARANCE | O.ACCESS<br>O.MANDATORY_ACCESS<br>O.MARKINGS<br>O.MANDATORY_INTEGRITY<br>O.USER_IDENTIFICATION |
| P.CRYPTOGRAPHY | O.ENCRYPTED_CHANNEL<br>O.ENCRYPTION_SERVICES<br>O.PROTECT<br>O.TSF_CRYPTOGRAPHIC_INTEGRITY |
| P.I_AND_A | O.USER_AUTHENTICATION<br>O.USER_IDENTIFICATION |
| P. INDEPENDENT_TESTING | O.PENETRATION_TEST<br>O.TESTING<br>O.VULNERABILITY_ANALYSIS |
| P.LABELED_OUTPUT | O.MARKINGS |

| | |
|---|---|
| P.NEED_TO_KNOW | O.ACCESS<br>O.DISCRETIONARY_ACCESS<br>O.DISCRETIONARY_USER_CONTROL<br>O.PROTECT<br>O.USER_IDENTIFICATION |
| P.REMOTE_ADMIN_ACCESS | O.ENCRYPTED_CHANNEL<br>O.ENCRYPTION_SERVICES<br>O.MANAGE<br>O.ADMIN_TRAINED<br>O.TRUSTED_PATH<br>O.TSF_CRYPTOGRAPHIC_INTEGRITY<br>O.USER_AUTHENTICATION<br>O.USER_IDENTIFICATION |
| P.RESOURCE_LABELS | O.MARKINGS |
| P.ROLES | O.MANAGE<br>O.ADMIN_TRAINED<br>O.TRAINED_USERS |
| P.SYSTEM_INTEGRITY | O.RECOVERY<br>O.SELF_PROTECTION<br>O.ADMIN_TRAINED<br>O.TRUSTED_SYSTEM_OPERATION<br>O.TSF_CRYPTOGRAPHIC_INTEGRITY |
| P.TRACE | O.AUDIT_REVIEW |
| P.TRUSTED_RECOVERY | O.RECOVERY |
| P.USER_CLEARANCE | O.MANDATORY_ACCESS<br>O.USER_IDENTIFICATION |
| P.VULNERABILITY_SEARCH | O.VULNERABILITY_ANALYSIS |

**P.ACCESS_BANNER -** *The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.*

This policy results in an objective to display advisory warnings (O.DISPLAY_BANNER).

**P.ACCOUNT -** *The users of the system shall be held accountable for their actions within the system.*

Enforcement of this policy requires that users be identified (O.USER_IDENTIFICATION), that their actions be monitored (O.AUDIT_GENERATION), and that the resulting records of their actions be available for review (O.AUDIT_REVIEW)

**P.AUTHORIZATION -** *The system must limit the extent of each user's abilities in accordance with the TSP.*

This policy requires that users in each of different roles (see P.ROLES) have a set of abilities defined according to the role, which restricts access to resources (O.ACCESS) and access to user data by users (O.PROTECT). Enforcing this policy requires the user to be identified (O.USER_IDENTIFICATION)

**P.AUTHORIZED_USERS -** *Only those users who have been authorized to access the information within the system may access the system.*

Enforcing this policy requires knowing who the user is (O.USER_IDENTIFICATION) and validating the claimed identity (O.USER_AUTHENTICATION).

**P.CLEARANCE -** *The system must limit the access to the information in protected resources to those authorized users whose clearance level is appropriate for the labeled data.*

Enforcing this policy requires the data be labeled (O.MARKINGS) and users each be assigned authorization levels (O.USER_IDENTIFICATION). These are then used in the enforcement of the label-based security policies (O.MANDATORY_ACCESS, O.MANDATORY_INTEGRITY O.ACCESS).

**P.CRYPTOGRAPHY -** *The system shall use NIST FIPS validated cryptography (methods and implementations) for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).*

This policy requires the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE [O.ENCRYPTION_SERVICES, O.ENCRYPTED_CHANNEL, O.PROTECT, O.TSF_CRYPTOGRAPHIC_INTEGRITY] and may be available for users and applications.

**P.I_AND_A -** *All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.*

This policy requires users to claim (O.USER_IDENTIFICATION) and verify (O.USER_AUTHENTICATION) an identity.

**P.INDEPENDENT_TESTING -** *The operating system must undergo independent testing as part of an independent vulnerability analysis.*

This policy requires that independent testing (O.TESTING) be performed in conjunction with a vulnerability analysis (O.VULNERABILITY_ANALYSIS) to demonstrate an adequate system design (O.PENETRATION_TEST).

**P.LABELED_OUTPUT -** *The beginning and end of all human-readable, paged, hardcopy output with sensitivity labels that properly represent the sensitivity of the output.*

The enforcement of this policy requires the data be labeled (O. MARKINGS).

**P.NEED_TO_KNOW -** *The system must limit the access to the information in protected resources to those authorized users who have a need to know that information.*

Enforcement of this policy requires the protection of resources (O.PROTECT) according to the rules of the discretionary access control policy (O.DISCRETIONARY_ACCESS), which controls access (O.ACCESS) based upon the identity of users (O.USER_IDENTIFICATION) as directed by the owner of the object (O.DISCRETIONARY_USER_CONTROL).

**P.REMOTE_ADMIN_ACCESS -** *Authorized administrators may remotely manage the IT operating system.*

For administrators to administer the system (O.MANAGE) remotely, there needs to be a protected communications path (O.ENCRYPTED_CHANNEL). Use of this path (O.ENCRYPTION_SERVICES) is restricted to authenticated (O.USER_AUTHENTICATION) administrators (O.USER_IDENTIFICATION), as described by the administrator guidance (O.ADMIN_TRAINED). The administrators also need a means of being certain that they are really communicating with the TSF (O.TRUSTED_PATH). Remote administrative actions require protection of the TSF data being transmitted to and from the TOE (O.TSF_CRYPTOGRAPHIC_INTEGRITY).

**P.RESOURCE_LABELS -** *All resources must have associated with them a label identifying the sensitivity level of data contained therein*

The enforcement of this policy requires the data be labeled (O. MARKINGS).

**P.ROLES -** *The authorized administrator and cryptographic administrator shall have separate and distinct roles associated with them.*

This policy requires there be separate roles, as described by the guidance directed to the user (O.TRAINED_USERS) and to the administrator (O.MANAGE, O.ADMIN_TRAINED).

**P.SYSTEM_INTEGRITY -** *The system must have the ability to periodically validate its correct operation and, with the help of administrators, it must be able to recover from any errors that are detected.*

This policy requires that the TOE recover to a safe state (O.RECOVERY), either periodically by itself or as directed by administrators (O.ADMIN_TRAINED) in order to maintain its security (O.TRUSTED_SYSTEM_OPERATION). This ensures that the TSF protects itself (O.SELF_PROTECTION). This validation is also done upon the cryptographic module (O.TSF_CRYPTOGRAPHIC_INTEGRITY)

**P.TRACE -** *The operating system must have the ability to review the actions of individuals.*

Audit events that have been generated must be able to be examined (O.AUDIT_REVIEW).

**P.TRUSTED_RECOVERY -** *Procedures and/or mechanisms shall be provided to assure that, after a system failure or other discontinuity, recovery without a protection compromise is obtained*

This policy requires that the TOE be able to recover itself to a safe state (O.RECOVERY).

**P.USER_CLEARANCE -** *All users must have associated with them a clearance level identifying the maximum sensitivity level of data that may be accessed.*

This policy requires that each user (O.USER_IDENTIFICATION) be associated with a clearance level (O.MANDATORY_ACCESS).

**P.VULNERABILITY_SEARCH -** *The system must undergo an analysis for vulnerabilities beyond those that are obvious.*

This policy requires that there be a vulnerability analysis (O.VULNERABILITY_ANALYSIS).

## 7.3 Objectives derived from Assumptions

55 Each of the identified security assumptions implies a set of security objectives to be met. The table below summarizes this mapping; this is then followed by explanatory text of how this mapping was derived for each assumption.

**Table 7.3 – Mapping of Security Objectives to Assumptions**

| Assumptions | Objectives enforcing Assumptions |
|---|---|
| A.PHYSICAL | OE.PHYSICAL |

**A.PHYSICAL -** *It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information.*

Physical security must be provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information. [OE.PHYSICAL]

## 7.4 Requirements Rationale

56 Each of the security objectives identified in sections 7.1 and 7.2 are met by a set of security requirements. The table below summarizes this mapping; this is then followed by explanatory text of how the mapping was derived.

**Table 7.4 – Mapping of Security Requirements to Objectives**

| Objectives from policies/threats | Requirements meeting objectives |
|---|---|
| O.ACCESS | FDP_ACC.2, FDP_ACF_US_INTERP_EXP.1, FDP_ETC.2, FDP_IFC.2, FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2), FDP_IFF.3, FIA_AFL_US_INTERP_EXP.1, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA_EXP.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FMT_REV.1(1), FMT_REV.1(2), FMT_SAE.1, FPT_RVM.1, FTA_SSL.1, FTA_SSL.2, FTA_TAB.1 |
| O.ACCESS_HISTORY | FTA_TAH.1 |
| O.ADMIN_ROLE | FMT_SMR.1, FMT_SMR.3 |
| O.ADMIN_TRAINED | ADO_DEL.2, ADO_IGS.1, AGD_ADM.1 |

| | |
|---|---|
| O.AUDIT_GENERATION | FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FAU_SEL.1, FIA_USB_US_INTERP_EXP.1, FMT_MOF.1, FPT_STM.1<br><br>ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1 |
| O.AUDIT_PROTECTION | FAU_SAR.2, FAU_STG.1, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)<br><br>ADV_SPM.1 |
| O.AUDIT_REVIEW | FAU_ARP.1, FAU_SAR.1, FPT_STM.1<br><br>ADV_FSP.2, ADV_HLD.2, ADV_SPM.1 |
| O.CONFIG_MGMT | ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ALC_DVS.1, ALC_FLR.2, ALC_LCD.1, ALC_TAT.1 |
| O.DISCRETIONARY_ ACCESS | FDP_ACC.2, FDP_ACF_US_INTERP_EXP.1, FDP_ITT.1, FIA_USB_US_INTERP_EXP.1, FMT_MSA.1(1), FMT_MSA.3, FMT_MSA_EXP.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FMT_REV.1(1), FMT_REV.1(2), FPT_RVM.1<br><br>ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1 |
| O.DISCRETIONARY_USER_CONTROL | FDP_ACF_US_INTERP_EXP.1 |
| O.DISPLAY_BANNERS | FIA_UAU.1, FIA_UID.1, FTA_TAB.1 |
| O.ENCRYPTED_CHANNEL | FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FPT_ITT.1, FTP_TRP.1 |
| O.ENCRYPTION_SERVICES | FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_CKM_EXP.1, FCS_CKM_EXP.2, FCS_BCM_EXP.1, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP_EXP.1, FIA_USB_US_INTERP_EXP.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FPT_ITT.1, FPT_ITT.3, FPT_TST.1(2), FPT_TST.1(3)<br><br>ADV_FSP.2, ADV_HLD.2, ADV_IMP.2, ADV_INT.1, ADV_LLD.1, ADV_SPM.1 |
| O.INSTALL | ADO_DEL.2, ADO_IGS.1 |

| | |
|---|---|
| O.MANAGE | FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.4, FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM_EXP.1, FCS_CKM_EXP.2, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4). FCS_COP_EXP.1, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2, FMT_MSA.3, FMT_MSA_EXP.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FMT_SAE.1, FPT_TST.1(1), FPT_TST.1(2), FPT_TST.1(3)<br><br>ADO_DEL.2, ADO_IGS.1, AGD_ADM.1 |
| O.MANDATORY_ACCESS | FDP_ETC.2, FDP_IFC.2, FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF.3, FDP_ITC.1, FDP_ITC.2, FDP_ITT.1, FIA_USB_US_INTERP_EXP.1, FMT_MSA.1(2), FMT_REV.1, FPT_RVM.1<br><br>ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1 |
| O.MANDATORY_INTEGRITY | FDP_ETC.2, FDP_IFC.2, FDP_IFF_US_INTERP_EXP.2(2), FDP_ITC.1, FDP_ITC.2, FDP_ITT.1, FIA_USB_US_INTERP_EXP.1, FMT_MSA.1(3), FMT_REV.1, FPT_ITT.3, FPT_RVM.1<br><br>ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1 |
| O.MARKINGS | FDP_ETC.2, FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2), FDP_ITC.1, FDP_ITC.2, FIA_ATD.1, FIA_USB_US_INTERP_EXP.1, FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2, FMT_MTD.1, FMT_REV.1, FPT_TDC.1 |
| O.PENETRATION_TEST | ATE_IND.2, AVA_CCA_EXP.1, AVA_MSU.1, AVA_SOF.1, AVA_VLA.3 |
| O.PROTECT | FDP_ACF_US_INTERP_EXP.1, FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2), FDP_ITC.2, FDP_ITT.1, FDP_RIP.2, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA_EXP.1, FMT_REV.1(1), FMT_REV.1(2), FPT_RVM.1, FPT_SEP.2, FTA_SSL.1, FTA_SSL.2 |
| O.RECOVERY | FPT_RCV.1, FPT_STM.1, FPT_TRC.1 |
| O.RESIDUAL_INFORMATION | FCS_CKM.4, FCS_CKM_EXP.2, FDP_RIP.2, FPT_RCV.1, FTA_SSL.1, FTA_SSL.2 |
| O.RESOURCE_SHARING | FRU_RSA.1(1), FRU_RSA.1(2) |

| | |
|---|---|
| O.SELF_PROTECTION | FAU_SAR.2, FAU_STG.1, FDP_ACF_US_INTERP_EXP.1, FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2), FDP_IFF.3, FDP_RIP.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FMT_REV.1(1), FMT_REV.1(2), FMT_SMR.1, FPT_AMT.1, FPT_ITT.1, FPT_ITT.3, FPT_RCV.1, FPT_RVM.1, FPT_SEP.2, FPT_TDC.1, FPT_TST.1(1), FPT_TST.1(2), FPT_TST.1(3) |
| O.SOUND_DESIGN | FPT_TST.1(2) FPT_TST.1(3), ALC_DVS.1, ALC_FLR.2, ALC_LCD.1, ALC_TAT.1, AVA_CCA_EXP.1, AVA_MSU.1, AVA_SOF.1, AVA_VLA.3, ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1 |
| O.SOUND_IMPLEMENTATION | FPT_TST.1(2), FPT_TST.1(3), ALC_DVS.1, ALC_FLR.2, ALC_LCD.1, ALC_TAT.1, ATE_COV.1, ATE_DPT.2, ATE_FUN.1, ATE_IND.2, AVA_CCA_EXP.1, AVA_MSU.1, AVA_SOF.1, AVA_VLA.3, ADV_FSP.2, ADV_HLD.2, ADV_IMP.2, ADV_INT.1, ADV_LLD.1, ADV_RCR.1 |
| O.TESTING | FPT_TST.1(2), FPT_TST.1(3), ATE_COV.2, ATE_DPT.2, ATE_FUN.1, ATE_IND.2 |
| O.TRAINED_USERS | AGD_USR.1 |
| O.TRUSTED_PATH | FTP_TRP.1 |
| O.TRUSTED_SYSTEM_OPERATION | FCS_COP_EXP.1, FIA_AFL_US_INTERP_EXP.1, FIA_UAU.7, FIA_UID.1, FMT_SAE.1, FPT_AMT.1, FPT_RCV.1, FPT_STM.1, FPT_TDC.1, FPT_TRC.1, FPT_TST.1(1), FPT_TST.1(2), FPT_TST.1(3), FTA_TAH.1, FTP_TRP.1<br><br>ADO_DEL.2, ADO_IGS.1, AGD_ADM.1 |
| O.TSF_CRYPTOGRAPHIC_INTEGRITY | FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM_EXP.1, FCS_CKM_EXP.2, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FPT_ITT.3, FPT_STM.1, FPT_TDC.1, FPT_TRC.1, FTP_TRP.1 |
| O.USER_AUTHENTICATION | FIA_SOS.1, FIA_UAU.1, FMT_MOF.1, FMT_MSA.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6), FMT_SAE.1, FTA_SSL.1, FTA_SSL.2, FTP_TRP.1<br><br>ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1 |

| | |
|---|---|
| O.USER_IDENTIFICATION | FIA_ATD.1, FIA_UID.1, FIA_USB_US_INTERP_EXP.1, FMT_SAE.1, FMT_SMR.1, FMT_SMR.3, FTP_TRP.1<br>ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1 |
| O.VULNERABILITY_ANALYSIS | FMT_MSA.3<br>AVA_CCA_EXP.1, AVA_MSU.1, AVA_SOF.1, AVA_VLA.3 |

**O.ACCESS -** *The IT operating system will ensure that users gain only authorized access to it and to its resources that it controls.*

The system permits access to itself and its resources only [FPT_RVM.1] according to its access control and integrity control policies [FDP_ACC.2, FDP_ACF_US_INTERP_EXP.1, FDP_IFC.2, FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2), FDP_IFF.3]. These policies compare attributes of users [FIA_UAU.1, FIA_UID.1]. User access to the system requires notification of proper use beforehand [FTA_TAB.1], and requires reauthentication [FTA_SSL.2] when the connection is idle for too long [FTA_SSL.1]. Only administrators [FIA_AFL_US_INTERP_EXP.1] may access administrative resources [FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA_EXP.1] and data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)]. Access remains until it is revoked [FMT_REV.1(1), FMT_REV.1(2)] or until attributes used to determine access are changed [FMT_SAE.1].

**O.ACCESS_HISTORY -** *The system will display information (to authorized users) related to previous attempts to establish a session.*

Information about previous sessions is displayed to the user [FTA_TAH.1].

**O.ADMIN_ROLE -** *The operating system will provide an administrator role to isolate administrative actions.*

The system will maintain roles to isolate administrative actions to authorized administrators [FMT_SMR.1, FMT_SMR.3].

**O.ADMIN_TRAINED -** *The IT operating system will provide authorized administrators with the necessary information for secure management.*

The administrator's procedures for the secure delivery [ADO_DEL.2], installation [ADO_IGS.1], and administration [AGD_ADM.1] of the TOE must be documented.

**O.AUDIT_GENERATION -** *The IT operating system will provide the capability to detect and create records of security relevant events associated with users.*

Security-relevant actions must be defined, auditable [FAU_GEN.1], and capable of being associated with individual users [FIA_USB_US_INTERP_EXP.1]. The audit records must be generated according to attributes [FAU_SEL.1] chosen by the administrator [FMT_MOF.1]. The associated time stamp must be

reliable [FPT_STM.1]. The audit system must detect possible security violations [FAU_SAA.1] and alert the administrator when they occur [FAU_ARP.1].

The audit mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The audit policy [ADV_SPM.1] is also defined.

**O. AUDIT_PROTECTION -** *The IT operating system will provide the capability to protect audit information.*

The audit trail must be protected so that only authorized users may access it [FAU_SAR.2]. Administrative functions must be available to do so [FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)]. The audit trail must be complete [FAU_STG.1]. The audit policy [ADV_SPM.1] includes a description of the protection of audit data.

**O. AUDIT_REVIEW -** *The IT operating system will provide the capability to selectively view audit information.*

An authorized administrator must be able to review [FAU_SAR.1] audit records and alarms based upon its contents [FAU_ARP.1]. Records must be able to be sorted by occurrence [FPT_STM.1], so that events can be recreated.

The audit policy [ADV_SPM.1] includes a description of the facilities available at the interface [ADV_HLD.2] to review audit data [ADV_FSP.2].

**O.CONFIG_MGMT -** *All changes to the operating system and its development evidence will be tracked and controlled.*

Versions of the TOE must be tracked [ACM_SCP.2] to prevent unwise changes from being introduced during its development. The automated system [ACM_AUT.1] will track the TOE and its associated documentation [ACM_CAP.4], along with any security flaws that are discovered during development. The TOE is developed according to a life-cycle model [ALC_LCD.1]. Security measures used during the development and maintenance of the TOE [ALC_DVS.1] will be documented, along with tools used during development [ALC_TAT.1] and procedures for remediating flaws discovered during maintenance [ALC_FLR.2].

**O.DISCRETIONARY_ACCESS -** *The IT operating system will control accesses to resources based upon the identity of users and groups of users.*

Discretionary access control must have a defined scope of control [FDP_ACC.2]. The rules of the DAC policy must be defined [FDP_ACF_US_INTERP_EXP.1]. The security attributes of objects [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)] and subjects [FIA_USB_US_INTERP_EXP.1] used to enforce the DAC policy [FPT_RVM.1] must be defined. This access control extends to objects from remote TOEs [FDP_ITT.1]. Authorized users must be able to control who has access to objects [FMT_MSA.1(1), FMT_MSA_EXP.1] and be able to revoke that access [FMT_REV.1(1), FMT_REV.1(2)]. Protection of named objects must be continuous, starting from object creation [FMT_MSA.3].

The discretionary access control mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The discretionary access control policy [ADV_SPM.1] is also defined.

**O.DISCRETIONARY_USER_CONTROL -** *The IT operating system must allow authorized users to specify which resources may be accessed by which users and groups of users.*

Owners of objects and administrators [FDP_ACF_US_INTERP_EXP.1] can change the object's attributes used for the enforcement of the discretionary access control policy.

**O.DISPLAY_BANNERS -** *The system will display an advisory warning regarding use of the TOE.*

Before users identify and authenticate themselves to the system, there is a message describing correct use [FTA_TAB.1]. These messages may be implemented as public objects where all users are allowed read access before authenticating [FIA_UAU.1, FIA_UID.1].

**O.ENCRYPTED_CHANNEL -** *Encryption will be used to provide confidentiality of TSF protected data in transit to remote parts of the TOE.*

The encryption operations [FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4)] support the secure transfer of TSF data between physically separate parts of the TOE [FPT_ITT.1]. The same kind of channel may also be used to implement the communications path between users and the TOE [FTP_TRP.1].

**O.ENCRYPTION_SERVICES -** *The IT operating system will make encryption services available to authorized users and/or user applications, as well as to the TSF.*

Cryptographic operation [FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP_EXP.1] and key management services [FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_CKM_EXP.1, FCS_CKM_EXP.2] are used to provide FIPS PUB 140-1 complaint encryption services [FCS_BCM_EXP.1] within the intended DoD environments. Keys are associated with users [FIA_USB_US_INTERP_EXP.1] and are managed by the cryptographic administrator [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)]. The cryptographic module supporting these services is periodically tested [FPT_TST.1(2), FPT_TST.1(3)] to be sure it is working correctly. TSF data must be protected in transit [FPT_ITT.1] and shall be able to detect modification and substitution of data [FPT_ITT.3].

The cryptographic module is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The architectural description [ADV_IMP.2] includes among its modules the cryptographic module, which must be designed so that it runs in a domain separate from the other modules [ADV_INT.1]. Any encryption policy must be described [ADV_SPM.1].

**O.INSTALL -** *The IT operating system will be delivered with the appropriate installation guidance to establish and maintain IT security.*

The procedures for secure delivery [ADO_DEL.2] and installation [ADO_IGS.1] of the TOE must be documented.

**O.MANAGE -** *The IT operating system will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the IT system.*

The administrator's procedures for the secure delivery [ADO_DEL.2], installation [ADO_IGS.1], and administration [AGD_ADM.1] of the TOE must be documented.

There must be a facility to audit security-relevant events [FAU_GEN.1, FAU_GEN.2, FAU_SEL.1], a means to review the audit records [FAU_SAR.1] in whole or selectively [FAU_SAR.3], and a means of managing a filled audit trail [FAU_STG.4]. There must be alarms that can be set to alert administrators to possible security violations [FAU_ARP.1], and a way to set the rules for defining what constitutes a security violation [FAU_SAA.1]. There must be self-tests of the TOE [FPT_TST.1(1)] and of the cryptographic module [FPT_TST.1(2), FPT_TST.1(3)].

There must be a means of administering the cryptographic services [FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP_EXP.1], and of managing the keys thereof [FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM_EXP.1, FCS_CKM_EXP.2].

There must be a means of managing security functions [FMT_MOF.1], TSF data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)], and security attributes [FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2, FMT_MSA.3, FMT_MSA_EXP.1], as well as a means address matters associated with the expiration of security attributes [FMT_SAE.1].

**O.MANDATORY_ACCESS -** *The IT operating system will control accesses to resources based upon the security level of users and resources.*

The mandatory access control policy [FDP_IFC.2] enforces rules [FPT_RVM.1] based upon attributes of users [FIA_USB_US_INTERP_EXP.1] and objects controlled by the TOE, as defined by rules [FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF.3] set by the administrator [FMT_MSA.1(2)]. This policy also covers objects exported [FDP_ETC.2] and imported [FDP_ITC.1, FDP_ITC.2] from/to the TOE as well as objects exchanged between separate parts of the TOE [FDP_ITT.1]. Access is revoked when the attributes are changed to remove access [FMT_REV.1].

The mandatory access mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The mandatory access control policy [ADV_SPM.1] is also defined.

**O.MANDATORY_INTEGRITY -** *The IT operating system will control accesses to resources based upon the integrity level of users and resources.*

The mandatory integrity policy [FDP_IFC.2] enforces rules [FPT_RVM.1] based upon attributes of users [FIA_USB_US_INTERP_EXP.1] and objects controlled by the TOE, as defined by rules [FDP_IFF_US_INTERP_EXP.2(2)] set by the administrator [FMT_MSA.1(3)]. This policy also covers objects exported [FDP_ETC.2] and imported [FDP_ITC.1, FDP_ITC.2] from/to the TOE as well as objects exchanged between separate parts of the TOE [FDP_ITT.1]. Access is revoked when the attributes are changed to remove access [FMT_REV.1]. The label of the user data is viewed as TSF data and must therefore be protected when the associated user data is transmitted [FPT_ITT.3].

The mandatory integrity mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The mandatory integrity control policy [ADV_SPM.1] is also defined.

**O.MARKINGS -** *The IT operating system will provide the capability to mark accurate sensitivity and integrity labels.*

Labels are used by the mandatory access and mandatory integrity policies [FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2),], both within the TOE and for objects exported [FDP_ETC.2] and imported [FDP_ITC.1, FDP_ITC.2] from/to the TOE. Labels are associated [FIA_USB_US_INTERP_EXP.1] with users [FIA_ATD.1] and are managed [FMT_MTD.1] by administrators [FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2]. There must also be consistent interpretation of the marking associated with TSF data shared between TOEs [FPT_TDC.1]. Changes in markings associated can result in revocation of access to that object [FMT_REV.1].

**O.PENETRATION_TEST -** *The operating system will undergo independent penetration testing to show to show that the system design and implementation are not bypassable.*

The TOE must undergo independent testing [ATE_IND.2] based upon the vulnerability analyses. These analyses search covert channels in the cryptographic module [AVA_CCA_EXP.1] and for any vulnerabilities that might be caused by unclear documentation [AVA_MSU.1]. These analyses for vulnerabilities must be systematic and show that the TOE is resistant to attackers with a moderate attack potential [AVA_VLA.3]. The testing must also support any claims regarding the strength of the functions [AVA_SOF.1].

**O.PROTECT -** *The IT operating system will provide means to protect user data and resources.*

User data is protected by the discretionary access control [FDP_ACF_US_INTERP_EXP.1], mandatory access control, and mandatory integrity policies [FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2)]. This protection provides the separation of user data [FPT_SEP.2] is based upon attributes managed by the administrator [FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA_EXP.1], including the identity [FIA_UID.1] of authenticated users [FIA_UAU.1, FIA_UAU.7]. The degree of protection is based upon the strength of the secrets [FIA_SOS.1]. User accounts are protected by requiring reauthentication for idle sessions [FTA_SSL.1, FTA_SSL.2]. User data is prevented from lingering in resources that are serially shared between users [FDP_RIP.2]. Access is permitted only until it is revoked [FMT_REV.1(1), FMT_REV.1(2)]. User data may be exchanged between separate parts of a distributed TOE [FDP_ITT.1]. All forms of protection are always enforced [FPT_RVM.1].

**O.RECOVERY -** *Procedures and/or mechanisms will be provided to assure that recovery* is obtained *without a protection compromise*, such as system failure or discontinuity.

Safe recovery includes not only recovery to a safe state [FPT_RCV.1], but also an accurate replication of TSF data [FPT_TRC.1] across distributed parts of the TOE that may become disconnected from one another, in which case it is necessary to be able to ascertain which is the most up-to-date data [FPT_STM.1].

**O.RESIDUAL_INFORMATION -** *The IT operating system will ensure that any information contained in a protected resource is not released when the resource is reallocated.*

User data is prevented from lingering in resources that are serially shared between users [FDP_RIP.2]. Such measures must also be performed on the resources used to store cryptographic data [FCS_CKM.4, FCS_CKM_EXP.2]. These resources are cleared when the system comes up after a failure [FPT_RCV.1]. Reauthentication information is also prevented from disclosure [FTA_SSL.1, FTA_SSL.2].

**O.RESOURCE_SHARING -** *No user will block others from accessing resources.*

If no user can obtain exclusive access to all resources, then that user cannot lock others from accessing those resources [FRU_RSA.1(1), FRU_RSA.1(2)].

**O.SELF_PROTECTION -** *The operating system will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.*

Protection of the TSF consists of protecting the TSF data as it is transferred [FPT_ITT.1, FPT_ITT.3] and maintaining its consistency [FPT_TDC.1]. TSF data includes audit records [FAU_SAR.2, FAU_STG.1]. The security functions are protected from access by unauthorized people [FMT_MOF.1, FMT_MSA.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)]. Testing the underlying hardware [FPT_AMT.1], self-testing the TOE [FPT_TST.1(1)], and testing the cryptographic module [FPT_TST.1(2), FPT_TST.1(3)] contribute to this protection.

Protection of resources controlled by the TSF consists of enforcement of the discretionary access control [FDP_ACF_US_INTERP_EXP.1], mandatory access control, and mandatory integrity control policies [FDP_IFF_US_INTERP_EXP.2(1), FDP_IFF_US_INTERP_EXP.2(2), FDP_IFF.3], which permit accesses to individual [FMT_SMR.1] based upon security attributes [FMT_REV.1(1), FMT_REV.1(2)]. This protection also extends to resources used by untrusted subjects [FDP_RIP.2]. The discretionary access control policy is based upon authenticated [FIA_UAU.1] user identities [FIA_UID.1].

This separation [FPT_SEP.2] is always enforced [FPT_RVM.1]. Self-protection also includes prevention of the system from entering an insecure state after failure [FPT_RCV.1].

**O.SOUND_DESIGN -** *The design of the IT operating system will be the result of sound design principles and techniques, which are accurately documented.*

A sound design depends upon careful development [ALC_DVS.1] in a well-defined life-cycle model [ALC_LCD.1]. This includes everything from identifying the development tools used [ALC_TAT.1] to remediating any flaws discovered during maintenance [ALC_FLR.2].

The correspondences among the development documentation [ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1] must be documented [ADV_RCR.1]. Problems with the design of the cryptographic module can be found from its self-tests [FPT_TST.1(2), FPT_TST.1(3)] as well as from an analysis of covert channels [AVA_CCA_EXP.1]. System-level problems in the design can be detected by an analysis for any vulnerabilities that might be caused by unclear documentation [AVA_MSU.1]. These analyses for vulnerabilities must be systematic and show that the TOE is resistant to attackers with a moderate attack potential [AVA_VLA.3]. There must also be an analysis of the strength of the functions [AVA_SOF.1].

**O.SOUND_IMPLEMENTATION -** *The implementation of the IT operating system will be an accurate instantiation of its design.*

A sound implementation depends upon careful development [ALC_DVS.1] in a well-defined life-cycle model [ALC_LCD.1]. This includes everything from identifying the development tools used [ALC_TAT.1] to remediating any flaws discovered during maintenance [ALC_FLR.2].

The correspondences among the development documentation [ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_IMP.2, ADV_INT.1] must be documented [ADV_RCR.1]. Problems with the implementation of the cryptographic module can be found from its self-tests [FPT_TST.1(2), FPT_TST.1(3)] as well as from an analysis of covert channels [AVA_CCA_EXP.1]. System-level problems in the design can be detected by an analysis for any vulnerabilities that might be caused by unclear documentation [AVA_MSU.1]. These analyses for vulnerabilities must be systematic and show that the TOE is resistant to attackers with a moderate attack potential [AVA_VLA.3]. There must also be an analysis of the strength of the functions [AVA_SOF.1]. Testing – both that performed as part of the developer's testing effort [ATE_COV.1, ATE_DPT.2, ATE_FUN.1] as well as independent testing [ATE_IND.2] for vulnerabilities theorized by these analyses – also helps to reduce implementation flaws.

**O.TESTING -** *The operating system will undergo independent testing, based at least in part upon an independent vulnerability analysis and includes test scenarios and results.*

The TOE must undergo independent testing [ATE_IND.2] based upon the developer's test effort [ATE_FUN.1]. The developer's testing effort must show adequate coverage [ATE_COV.2] and depth [ATE_DPT.2] to be considered complete. Testing efforts must pay particular attention to the correct operation of the cryptographic module [FPT_TST.1(2), FPT_TST.1(3)].

**O.TRAINED_USERS -** *The IT operating system will provide authorized users with the necessary guidance for secure operation.*

The user's procedures for the secure use of the TOE [AGD_USR.1] must be documented.

**O.TRUSTED_PATH -** *The operating system will provide a means to ensure users are not communicating with some other entity pretending to be the operating system.*

A trusted path to the TOE must be available to the users [FTP_TRP.1].

**O.TRUSTED_SYSTEM_OPERATION -** *The IT operating system functions in a manner that maintains IT security.*

Maintaining security is also achieved through the periodic self-testing of the TOE [FPT_TST.1(1)], the underlying hardware [FPT_AMT.1], and especially the cryptographic module [FPT_TST.1(2), FPT_TST.1(3)]. Safe operation includes not only recovery to a safe state [FPT_RCV.1] when these tests detect an error, but also in accurate replication of TSF data throughout the TOE [FPT_TRC.1] or between TOEs [FPT_TDC.1]; in cases where inconsistency is detected, it is necessary to be able to be certain which is the most up-to-date data [FPT_STM.1].

Providing a trusted path [FTP_TRP.1] to users helps to ensure that they securely provide their identities and successfully authenticate themselves [FIA_UAU.7] to the TOE before any TSF-mediated actions [FIA_UID.1]; repeated incorrect authentication closes the account [FIA_AFL_US_INTERP_EXP.1].

Users must also be given their access histories [FTA_TAH.1] so they can be aware of any possible compromise of their accounts.

The correct operation of the cryptographic module depends upon random numbers [FCS_COP_EXP.1]. Any data attributes that could expire must be managed only by the personnel authorized to manage them [FMT_SAE.1].

The procedures for the secure delivery [ADO_DEL.2], installation [ADO_IGS.1], and administration [AGD_ADM.1] of the TOE must be documented.

**O.TSF_CRYPTOGRAPHIC_INTEGRITY -** *The IT operating system will provide cryptographic integrity mechanisms for TSF data while in transit to remote parts of the TOE.*

Cryptography may be used to protect TSF data as it is stored in the TOE [FPT_TRC.1], and as it is transmitted between parts of a physically-distributed TOE [FPT_ITT.3], or between TOEs [FPT_TDC.1]. It may also be used to implement a trusted path for the user [FTP_TRP.1], or to protect timestamped transmissions [FPT_STM.1]. The correct operation of the cryptography [FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4)] includes secure generation of the keys [FCS_CKM.1(1), FCS_CKM.1(2)] and maintained integrity of the keys while they are stored [FCS_CKM_EXP.1, FCS_CKM_EXP.2].

**O.USER_AUTHENTICATION -** *The operating system will verify the claimed identity of the user.*

Users must authenticate [FIA_UAU.1] their claimed identities (see O.USER_IDENTIFICATION) to the TOE via the trusted path [FTP_TRP.1]. This authentication information must exhibit certain characteristics [FIA_SOS.1], as determined by the administrator [FMT_MOF.1, FMT_MSA.2] who manages it [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_MTD.1(6)]. Administrators have to ability to give authentication information lifetimes, after which they must be changed [FMT_SAE.1]. Users are required to supply this information to reactivate idle sessions [FTA_SSL.1, FTA_SSL.2]

The authentication mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The authentication policy [ADV_SPM.1] is also defined.

**O.USER_IDENTIFICATION -** *The operating system will uniquely identify users*.

Users authorized to access the TOE identify themselves to the TOE [FIA_UID.1] via a trusted path [FTP_TRP.1], and then authenticate this claimed identity (see O.USER_AUTHENTICATION). Identified users have attributes [FIA_ATD.1] associated with them [FIA_USB_US_INTERP_EXP.1], which may include an association with one or more roles provided by the TOE [FMT_SMR.1, FMT_SMR.3]. These attributes may expire [FMT_SAE.1]

The identification mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The identification policy [ADV_SPM.1] is also defined.

**O.VULNERABILITY_ANALYSIS -** *The system will undergo an analysis for vulnerabilities beyond those that are obvious.*

Such vulnerabilities include the manipulation of the security attributes of newly created objects through which unauthorized access may be gained [FMT_MSA.3]. A vulnerability analysis that searches for covert channels in the cryptographic module [AVA_CCA_EXP.1] must be documented. There must also be an analysis for any vulnerabilities that might be caused by unclear documentation [AVA_MSU.1]. These analyses for vulnerabilities must be systematic and show that the TOE is resistant to attackers with a moderate attack potential [AVA_VLA.3]. There must also be an analysis of the strength of the functions [AVA_SOF.1].

## 7.5 Explicit Requirements Rationale

57 The following explicit requirements have been included in this Protection Profile because the Common Criteria requirements were found to be insufficient as stated. For the US CC interpretations (components ending in "_US_INTERP_EXP"), the rationale column only contains the rationale for the actual element changed in the interpretation.

58 Explicit Functional Requirements

**Table 7.5 – Rationale for Explicit Functional Requirements**

| Explicit Component | Rationale |
|---|---|
| FCS_CKM_EXP.1 | The CC cryptographic support section does not specifically address the concepts of key validation techniques and key packaging. Although closely tied to generated keys, these concepts typically get implemented just after, not during, the actual generation of a key.<br><br>In this PP, FCS_CKM_EXP.1 allows for specifically addressing these key management-related concepts. |
| FCS_CKM_EXP.2 | The CC does not provide components for key handling and storage. Key access and key destruction components do not address keys being transferred within the device nor key archiving when key is not in use.<br><br>FCS_CKM_EXP.2 addresses internal key transfer and archiving. It also addresses the handling of storage areas where keys reside. |
| FCS_BCM_EXP.1 | The CC does not provide a means to specify a cryptographic baseline of implementation.<br><br>FCS_BCM_EXP.1 provides for the specification of the required FIPS certification based on the implementation baseline. |
| FCS_COP_EXP.1 | The CC cryptographic operation components are focused on specific algorithm types and operations requiring specific key sizes.<br><br>The generation of random numbers can be better stated as an explicit component. Neither algorithms nor keys are required to generate random numbers. Random number generators can use any combination of software-based or hardware-based inputs as long as the required RNG/PRNG tests are successful. |

| | |
|---|---|
| FDP_ACF_US_INTERP_EXP.1 | The CC wording for FDP_ACF.1.1 is unclear when it refers to an assignment of "security attributes, named groups of security attributes": This is unclear in that it seems to call for a simple list of security attributes, without association of security attributes to the controlled entities.<br><br>This interpretation corrects this problem. It makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This can be clearly provided as a two column table: one column is the controlled entity (subject, information), the other is a list of SFP-relevant security attributes for that controlled entity. |
| FDP_IFF_US_INTERP_EXP.2[27] | The CC wording for FDP_IFF.2.1 and FDP_IFF.2.2 is confusing and unclear when it refers to an assignment of "the minimum number and type of security attributes":<br>This is confusing in the area of "minimum number"; the annex fails to clarify this when it refers to a "minimum number...to support the environmental needs".<br>This is unclear in that it seems to call for a simple list of security attributes, without association of security attributes to the controlled entities.<br>This interpretation corrects this problem. It makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This can be clearly provided as a two column table: one column is the controlled entity (subject, information), the other is a list of SFP-relevant security attributes for that controlled entity. |

[27] Rationale is the same for both iterations.

| | |
|---|---|
| FIA_AFL_US_INTERP_EXP.1 | The Part 2 Annex for FIA_AFL says, for the assignment:<br><br>In FIA_AFL.1.1, if the PP/ST author should specify the default number of unsuccessful authentication attempts that, when met or surpassed, will trigger the events. The PP/ST author may specify that the number is: "an authorized administrator configurable number".<br><br>This is reasonable; the PP/ST author may wish to allow the number to be adjusted dynamically by an authorized administrator. However, the wording used ("[assignment: number]") does not allow a phrase to be inserted. This interpretation permits the phrase.<br><br>This interpretation also addresses an ambiguity in the original words. "Number", as used in the element, could potentially be real or negative. That is inappropriate; it is more precise to call it a positive integer. |
| FIA_UAU_EXP.1 | The CC does not contain specific requirements to articulate proper verification of the authorized user's identity.<br><br>FIA_UAU_EXP.1 prevents short cuts to the authentication mechanism that would allow a person to login by entering an incorrect password (that contains the correct password within but is not entirely correct). |

| | |
|---|---|
| FIA_USB_US_INTERP_EXP.1 | At the time a PP/ST is developed, the PP/ST author knows the significant attributes of the FSPs of the TOE, and which of those attributes are to be derived from user-based information. Thus, it is possible for the PP/ST author to specify which user attributes are to be bound to subjects created on the user's behalf.<br><br>However, in CC v2.1, the words of the FIA_USB.1.1 element use the word "appropriate". In order to specify the specific attributes to be bound, the PP/ST author must refine the element, and the evaluator must determine if the specified attributes are indeed "appropriate"; further, the evaluator must determine if there are appropriate attributes not included in the refined element. This creates a risk of inconsistent evaluator interpretation.<br><br>The ideal approach is to replace the need for refinement with an explicit assignment. The assignment should be driven by the attributes that are needed to enforce the TSP. For example, an access control policy based on user identity would require the user identity information be bound to the subject.<br><br>This interpretation should be distinguished from I-0353/I-0354, which discuss the security attributes bound to subjects, for not all subject security attributes derive from user attributes. |
| FMT_MSA_EXP.1 | The CC does not contain specific requirements to articulate management rules for security attributes of objects. FDP_ACF deals with rules of access control once attributes are set. It does not deal with the rules for setting these attributes.<br><br>FMT_MSA_EXP.1 allows for each access right that may be modified, the list of restrictions that exist for each type of user. |

### 7.5.1 Explicit Assurance Requirements

**Table 7.6 – Rationale for Explicit Assurance Requirements**

| Explicit Component | Rationale |
|---|---|
| AVA_CCA_EXP.1 | The CC does not have requirements to perform partial covert channel analysis on only the cryptographic elements.<br>AVA_CCA_EXP.1 provides for flexibility to focus covert channel analysis only upon the cryptographic module to search for leakage of critical security parameters. |

## 7.6 Rational for Strength of Function

59 The TOE minimum strength of function is SOF-medium. The evaluated TOE is intended to operate in DoD medium robustness environments processing up to DoD classified information. The minimum strength of function was chosen to be consistent with FIA_SOS.1 by providing a probability of successful authentication for a random attempt of less than one in $2.5 \times 10^{14}$. This security function is in turn consistent with the security objectives described in section 7.4.

60 The minimum SOF does not apply to any cryptographic mechanisms with respect to a CC evaluation. The strength of cryptographic algorithms is outside the scope of the CC. The strength of the cryptographic mechanisms will be determined by NIST FIPS 140-1 certification, the tests included in this PP, and the covert channel analysis on cryptographic module.

## 7.7 Rationale for Assurance Rating

61 This protection profile has been developed for a DoD medium robustness environment. The TOE environment and the value of information processed by this environment establish the need for the TOE to be evaluated at an Evaluated Assurance Level 4 Augmented (EAL4+)[28].

[28] Refer to the "Mutual Recognition of Common Criteria Certificates" section 1.3 to read conditions for the CC certificate to be mutually recognized for PPs with EALs higher than 4.

# 8. References

[1] Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation, CCIB-98-026, Version 2.1, August 1999

[2] Department of Defense Chief Information Officer, Guidance and Policy for Department of Defense Information Assurance Memorandum No. 6-8510 dated 16 June 2000

[3] National Institute of Standards and Technology, Data Encryption Standard (DES); specifies the use of Triple DES, Federal Information Processing Standard Publication (FIPS-PUB) 46-3, dated November 1999 (http://www.csrc.nist.gov/fips/fips46-3.pdf)

[4] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standard Publication (FIPS-PUB) 186-2, dated February 2000 (http://csrc.nist.gov/fips/fips186-2.pdf)

[5] National Institute of Standards and Technology, Key Management Using ANSI X9.17, Federal Information Processing Standard Publication (FIPS-PUB) 171, dated April 1992 (http://csrc.nist.gov/fips/fips171.txt)

[6] National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standard Publication (FIPS-PUB) 180-1, dated April 1995 (http://www.itl.nist.gov/fipspubs/fip180-1.htm)

[7] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standard Publication (FIPS-PUB) 140-1, dated January 11, 1994 (http://www.itl.nist.gov/fipspubs/fip140-1.htm)

[8] National Security Agency, Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999

[9] National Security Agency, Information Assurance Technical Framework (IATF), Version 2.0.1 - September 1999 (http://www.iatf.net/)

[10] Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria (Orange Book), December 1985

[11] Trusted Product Evaluation Program (TPEP) Trusted Computer System Evaluation Criteria (TCSEC) Interpretations

[12] National Security Agency, Labeled Security Protection Profile (LSPP) Version 1.b, 8 October 1999

# Appendix A — Acronyms

| | |
|---|---|
| CC | Common Criteria for Information Technology Security Evaluation Version 2.1 |
| COTS | Commercial Off-The-Shelf |
| CSP | Critical Security Parameters |
| DAC | Discretionary Access Control |
| DoD | Department of Defense |
| EAL | Evaluation Assurance Level |
| FIPS | Federal Information Processing Standard |
| GiG | Guidance and Policy for Department of Defense Information Assurance Memorandum No. 6-8510 |
| IA | Information Assurance |
| IT | Information Technology |
| MAC | Mandatory Access Control |
| MIC | Mandatory Integrity Control |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| SF | Security Function |
| SFP | Security Function Policy |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSFI | TSF Interface |
| TSP | TOE Security Policy |

# Appendix B — Cryptographic Standards, Policies, and Other Publications

**Standards**

| | |
|---|---|
| ANSI X9.42 | Agreement of Symmetric Keys Using Discrete Logarithm Cryptography |
| ANSI X9.44 | Public Key Cryptography for the Financial Services Industry: Key Establishment Using Factoring Based Public Key Cryptography |
| ANSI X9.63 | Public Key Cryptography for the Financial Service Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography |
| FIPS PUB 140-1 | Security Requirements for Cryptographic Modules |
| FIPS PUB 171 | Key Management Using ANSI X9.17 |
| FIPS PUB 180-1 | Secure Hash Standard |
| FIPS PUB 186-2 | Digital Signature Standard |
| FIPS PUB 46-3 | Data Encryption Standard (DES) |
| PKSC#11 | Cryptographic Token Interface Standard |
| PKSC#12 | Personal Information Exchange Syntax |
| PKSC#5 | Password-based Encryption Standard |
| PKSC#8 | Private-Key Information Syntax Standard |

**Policies**

X.509 Certificate Policy for the DOD

**Other Publications**

| | |
|---|---|
| NIST Special Publication 800-22 | A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications |

PKI Roadmap for the DOD