COTS Compartmentalized Operations Protection Profile – Operating Systems

(CCOPP-OS)

DEFINITIVE

Version 2.0
June 19, 2008

Sponsored by:

Hewlett-Packard.

Prepared by:

Hewlett-Packard.

This document is consistent with the
Common Criteria for Information Technology Security Evaluation
Version 3.1 Revision 2

Interpretations Incorporated (as applicable)
CCMB
All approved posted to http://www.commoncriteriaportal.org as of 6/19/08

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

1.1 IDENTIFICATION

Title: CCOPP-OS - COTS Compartmentalized Operations Protection Profile - Operating Systems

Registration: <To be filled in upon registration>

Keywords: Protection Profile, Commercial, COTS, Compartmentalized Mode, Compartmentalized Operations, operating system, compartmentalized, access control, information protection, role based, discretionary, mandatory, separation of duties, non-discretionary.

1.2 CONFORMANCE CLAIMS

The CCOPP-OS is:

- CC Part 2 Extended
- CC Part 3 Conformant
- EAL4 Conformant
- Conformant with the Controlled Access Protection Profile (CAPP) [CAPP] and the Role Based Access Control (RBAC) Protection Profile [RBAC].

Common Criteria Version 3.1 Revision 2 [CC-V3.1] has been used to develop this PP.

1.3 CONFORMANCE STATEMENT

Conformance to the CCOPP-OS shall be **demonstrable**, as defined in CC Part 1.

1.4 PURPOSE

The purpose of CCOPP-OS is to define, and specify the requirements necessary to solve, the security problem that organizations encounter when trying to implement readily available operating systems (perhaps with add-on packages) to handle compartmentalized environments working within the same operating system.

This PP has been developed using guidance from [CSPP-OS], with many thanks to Gary Stoneburner, formerly of NIST and now at APL, for his efforts.

This PP also is a superset of both [CAPP] and [RBAC], which have been incorporated into this document. It also contains much of the [LSPP]. We wish to offer many thanks to NSA and NIST.

1.5 GLOSSARY OF TERMS

Unless otherwise specified, all terms are as defined in the CC. This section is intended to meet the CC requirement APE_REQ.2.2C; however, given that a PP is by its very nature generic, these definitions are also generic. Specific definitions can only be given in the CCOPP-OS conformant ST, which relates to a specific TOE.

Active Role Set: This is the subset of the set of authorized roles for a user that has actually been activated for the user in a particular user session. The total set of access rights (privileges) available to a user in a session is the sum of the access rights directly assigned to each member of the Active Role Set together with the privileges inherited by each member of the Active Role Set through roles assigned to it. (See also *Default Active Role Set*.)

Default Active Role Set: Instead of forcing the user to build an Active Role Set during every user session, the RBAC administrator provides a default set of roles (from the list of authorized roles for the user). The composition of the Default Active Role Set determines the initial available access rights for the user at the start of the session. In other words, the Default Active Role Set is the Active Role Set at the time of session creation. In many software environments the user may be able to change the composition of this Active Role Set during the course of the user session.

Named Object: An object that is 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.

Object: CC defines this term as "a passive entity in the TOE, that contains or receives information, and upon which subjects perform operations". For a CCOPP-OS conformant TOE, this will typically include files, file containers (e.g. directories or folders), and also such entities as inter-process communications objects.

Operation: CC defines this term as "a specific type of action performed by a subject on an object". For a CCOPP-OS conformant TOE, operations will generally be dependent on the type of object in question, but typically will include such actions as "create", "read", "modify", "delete", and (where relevant) "execute".

Security attribute: CC defines this term as "a property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs". For a CCOPP-OS conformant TOE, these include:

- For users and subjects: user identity, user group(s), and role(s), and compartment label(s) for that user

- For objects: DAC and RBAC permissions or Access Control Lists, and compartment label(s) used to enforce the MAC policy.

Subject: CC defines this term as "an active entity in the TOE that performs operations on objects". For a CCOPP-OS conformant TOE this will typically be a user process.

2. TOE OVERVIEW

The Target of Evaluation (TOE) in a Common Criteria Protection Profile is the information technology component or system for which requirements are to be specified. This chapter describes the CCOPP-OS in terms of the type of TOE covered by the PP.

2.1 TOE TYPE AND BOUNDARY

CCOPP-OS covers Compartmentalized Operations operating systems in both stand-alone and networked environments. The CCOPP-OS conformant TOE permits one or more processors and attached peripherals and storage devices to be used by users to perform a variety of functions requiring controlled, shared access to processing capability and information. In a networked environment, the TOE also permits interfaces among distributed systems to be used by users.

The TOE will provide user services directly or serve as a platform for networked applications and will support communications across an appropriately protected network.

As a minimum, the TOE boundary encompasses the operating system software. The following components form an essential part of the IT environment:

- One or more add-on packages to increase the base functionality by providing additional authentication mechanisms (for which the TOE is required to provide support).

- The underlying hardware platform.

It should be noted that the CCOPP-OS does not preclude a conformant ST from drawing the TOE boundary differently, i.e. to include the additional authentication mechanisms and/or the hardware platform.

2.2 OPERATIONAL ENVIRONMENT

The TOE supports the active entities of human users and software processes. Human users, in conjunction with system processes, are accountable for all system activities. The TOE generates processes that act on behalf of either a specific human user or a uniquely identifiable system process. A process requests and consumes resources on behalf of its unique, associated user or system process. In a networked environment, a process may invoke another process on a different system.

The TOE is intended for use in both stand-alone and networked environments.

A conformant TOE will support:

- Users or processes with networked access to the TOE across an appropriately protected network (that is, mechanisms operating within the TOE cooperate with mechanisms in other components to securely exchange information across an appropriately protected network)

- Several users executing tasks on the same system concurrently

- Sharing resources, such as printer and mass storage, across a network.

CCOPP-OS conformant TOEs are *not* expected to:

- totally protect against malicious abuse of authorized privileges

- adequately protect against sophisticated attacks (including denial of service)

- provide sufficient protection against installation, operation, or administration errors.

Depending on the environment in which the TOE is deployed, a CCOPP-OS conformant TOE may need to implement additional security functions, not within the scope of CCOPP-OS, to protect user data when it is transmitted between different components of a networked TOE, or when exchanged with another trusted IT product within the IT environment.

2.2.1 Types of access and control

- **Authenticated users**:
    - Are uniquely identifiable by the system
    - Utilize highly-controlled privileges which are access rights associated with each process that control the capabilities of the process
    - Have legitimate access beyond publicly available information
    - Are authenticated prior to being granted such access.

- **Compartmentalization:** allows or denies access to resources by access control mechanisms that "label" access restrictions to the information.

- **Role-Based Access Control:** is a mechanism to map users to the permitted operations, by associating subjects to roles to operations.

2.2.2 Nature of intended use

A CCOPP-OS conformant TOE is suitable for the protection of information in real-world environments, subject to the limitations noted above.

- A CCOPP-OS conformant TOE is suitable for specifying the baseline protection requirements for information in environments where all authenticated users are either (1) trusted to not maliciously attempt to circumvent nor by-pass access controls or (2) lack the motivation or capability for sophisticated penetration attempts.

- The Mandatory Access Control (MAC) policy is a set of rules that determines access based upon the compartment (e.g., PERSONNEL, MEDICAL) of the subject and the object, and a label based access rule (also called label-based restrictions) on each object (e.g., READ from MEDICAL compartment, READ/WRITE from PERSONNEL compartment). The label based rule may be derived from the attributes of the object or environmental factors. Without loss of generality, this document assumes that the access rules of objects are represented as a set of (compartment-name, object compartment, access-mode) combinations.

- A CCOPP-OS conformant TOE shall support at least two site-definable compartments. It shall also support at least two access modes for one or more objects under TOE control.

2.3 SUMMARY OF SECURITY REQUIREMENTS

2.3.1 Assurance

CCOPP-OS assurance requirements have been selected to provide the level of confidence resulting from (1) existing recognized good practices for OS development and (2) an easily-identified process for third-party evaluation. This equates, in summary, to OS technical countermeasures that:

- are sufficient for controlling a community of authenticated users

- can provide protection against unsophisticated technical attacks

- can not be expected to provide sufficient protection against sophisticated, technical attacks (to include denial-of-service).

2.3.2 Security Functionality

The CCOPP-OS conformant TOE addresses these user needs:

- identification and authentication of users

- enforcing Discretionary Access Control (DAC) Policy between subjects and objects, which allows authorized users and authorized administrators to control access by subjects to objects on the basis of individual user identity or membership in a group.

- enforcing Mandatory Access Control (MAC) Policy between subjects and objects, which determines the access based on the compartment label(s) of subjects and objects that are assigned and changed by authorized administrators or TSF. Information flow control is enforced through MAC Policy at the compartment level. MAC Policy is appropriate in environments where regulatory or organizational policy requires the stored information to be protected from access by authenticated users who are not allowed access to such information.

- enforcing Role-Based Access Control (RBAC) Policy such that access to objects and the permitted operations with respect to them by subjects can only take place in accordance

with the role-based access restrictions placed on the objects by authorized administrators. RBAC Policy, through the separations of duties, enforces the least privileges.

- providing support for controlling access based upon environmental constraints such as time-of-day and port-of-entry.

- resistance to resource depletion by providing resource allocation features.

- providing mechanisms to detect and record security relevant events.

- providing mechanisms for trusted recovery in the event of most system failures or detected insecurities.

- supporting these capabilities in a distributed system connected via an appropriately protected network.

3. SECURITY PROBLEM DEFINITION

3.1 INTRODUCTION

This chapter identifies the following:

- assumptions about the operational environment for CCOPP-OS conformant TOEs

- organizational security policies for which CCOPP-OS conformant TOEs are appropriate

- threats to the assets requiring protection, to be countered by security functionality provided by the CCOPP-OS conformant TOE and/or controls within its operational environment.

This chapter thus provides the basis for derivation of the security objectives described in chapter 4 and hence the specific security requirements listed in chapters 5 and 6.

3.1.1 Assets

The IT assets requiring protection by the CCOPP-OS conformant TOE are the information it stores and processes, its resources, and the services it provides to authorized users. The value of the assets merits moderately intensive penetration or masquerading attacks.

3.1.2 Threat agents

Threat agents may be either authorized or unauthorized users of the TOE. Authorized users will vary in the degree of access rights and privileges they have been granted. In general, this security problem definition draws no distinction between different types of user; however, in certain specific instances the term *authorized administrator* is used to denote an individual who has been given responsibilities in respect of security administration of the TOE.

There are two broad categories of users with respect to these assumptions and threats:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, have some rights of access, and are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.

- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. CCOPP-OS conformant TOEs would generally be used in environments where these users are highly trusted not to attempt to maliciously subvert the system or to maliciously exploit the information stored thereon, or are restricted from gaining access by environmental measures.

3.2   ASSUMPTIONS ON THE OPERATIONAL ENVIRONMENT

The specific conditions listed below are assumptions on the operational environment.

The TOE is not expected to be able to sufficiently mitigate risks resulting from application of sophisticated attack methods. This is reflected in the definition of the assumptions on the operational environment, and also the statement of threats to be countered within that operational environment.

Table 3.2.1 – Assumptions on the operational environment: TOE usage

Name	Assumption	Discussion
A.COMPARTMENT	Procedures exist for establishing the compartment label based restrictions of all information imported into or stored in the system.	This is essential to ensure Compartmentalization controls are effective, so that users will only be able to access that information for which they have the privilege to see.
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.	This is essential to ensure that all assets are consistently protected throughout a distributed TOE, and that they will not be compromised when transferred to external systems. CCOPP-OS conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems. If, however, the conformant ST can demonstrate that there are other measures in place to ensure consistent protection of assets, this assumption may be relaxed or removed.

Table 3.2.2 – Assumptions on the operational environment: Physical

Name	Assumption	Discussion
A.LOCATE	The processing resources of the TOE and connections to peripheral devices will be located within controlled access facilities which will prevent unauthorized physical access. It is also assumed that physical controls in place would alert the system authorities to the physical presence of attackers within the controlled space.	It is essential to protect the machines and connections to devices from physical attack.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. Internal communication paths to access points such as terminals are assumed to be adequately protected.	It is essential to ensure that no unauthorized changes are made to the TOE hardware, or software or internal communication paths.

Table 3.2.3 – Assumptions on the operational environment: Personnel

Name	Assumption	Discussion
A.ACCESS	Rights for users to gain access and perform operations on information are based on their membership in one or more roles. These roles are granted to the users by the RBAC Administrator. These roles accurately reflect the users' job function, responsibilities, qualifications, and/or competencies within the enterprise.	This is fully explained in the assumption statement itself.
A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.	Cooperation in a normal environment is a necessary and expected situation.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	It is essential that the security of the information be managed in an efficient and secure manner.

Name	Assumption	Discussion
A.NO-EVIL-ADMIN	The system administrative personnel are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the administrative documentation.	It is essential that the administrative personnel be trusted, as the TOE can not protect against this type or attack.
A.USER-NEED	Authenticated users recognize the need for a secure IT environment.	It is essential that the authenticated users appreciate the need for security. Otherwise they are likely to try and circumvent it, e.g. "to get the job done".
A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	Authenticated users will be assigned a level of trust that is dependent on their access rights and privileges. However, this "trust" is not absolute, and hence the phrase "generally trusted".

3.3 ORGANIZATIONAL SECURITY POLICIES

The organizational security policies (OSPs) discussed below are to be addressed by the CCOPP-OS conformant TOE and its operational environment. OSPs are based on the operational standards and quality procedures of the organization hosting the TOE. A conformant TOE may thus need to comply with other policies that are not stated here, for example: government regulations, national and local laws, and contractual agreements; these will be specified in the Security Target for that TOE.

Table 3.3.1 – Organizational Security policies

Name	Policy	Discussion
P.ACCESS	Access rights by individual users to specific data objects are to be determined by the designated owner of the object, as laid down by the organization's security policy. These are to be based on the security attributes assigned to both the object and the individual user attempting access, as well as any environmental conditions that must also apply.	CCOPP-OS supports organizational policies which grant or deny access to objects using rules driven by attributes of the user (such as user identity, group, etc.), attributes of the object (such as permission bits), type of access (such as read or write), and environmental conditions (such as time-of-day or major plant (or unit) operating state), where this refers to whether the plant or unit is in "normal" operation, startup/shutdown, or a formally declared emergency.
P.ACCOUNTABILITY	Users are to be held accountable for their security-relevant actions.	CCOPP-OS supports organizational policies requiring that users are held accountable for their actions, facilitating after-the-fact investigations and providing some deterrence to improper actions.
P.AUTHORIZED-USER	Only those individuals who have been authorized to access the information within the system are to be able to access the system.	This is well-defined in the description.

Name	Policy	Discussion
P.COMPARTMENT	Access by individuals to information is to be restricted, based on the compartment label of the individual and the label-based access restrictions of the information. The access rules enforced are to prevent individuals from accessing information to which they are not authorized, in accordance with established information flow control policies.	This is well-defined in the description.
P.NEED-TO-KNOW	Access to information, and the ability to modify or destroy that information, is to be limited to those authorized individuals who have a "need to know" for that information.	The method for compartmentalization of information is made based on criteria set forth by the owning organization. This is usually done on a basis of relative value to the organization and its interest to limit dissemination of that information. The determination of compartmentalization of information is outside the scope of the TOE, which is only expected to enforce the compartmentalization rules that have been defined.
P.TRAINING	Authorized users are to be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies.	Once granted legitimate access, authenticated users are expected to use IT resources and information only in accordance with the organizational security policy. In order for this to be possible, these users must be adequately trained both to understand the purpose and need for security controls and to be able to make security decisions with respect to their discretionary actions.
P.USAGE	The organization's IT resources are to be used only for authorized purposes.	The CCOPP-OS conformant TOE, in conjunction with its environment, ensures that the organization's information technology is not used for unauthorized purposes. (This Policy will be addressed by written Corporate Polices, not by the TOE).

3.4   THREATS TO SECURITY

The TOE and its operational environment are required to counter threats which may be broadly categorized as:

- the threat of unsophisticated, malicious attacks from individuals other than authenticated users

- the threat of authenticated users attempting, non-maliciously to gain unauthorized access or to perform an unauthorized operation. Such attempts may be performed to "get the job done", out of curiosity, as a challenge, or as a result of an error.

The specific threats to be countered are listed in Tables 3.4.1 and 3.4.2.

Table 3.4.1 – Threats addressed by the TOE supported by its operational environment

Name	Threat
T.ACCESS	An authenticated user may gain unauthorized, non-malicious access to the TOE or a resource or to information directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.
T.CRASH	The secure state of the TOE could be compromised in the event of a system crash, leading to corruption or loss of assets.
T.DENIAL	The TOE may be subjected to an unsophisticated, denial-of-service attack.
T.ENTRY	An individual, other than an authenticated user, may gain unauthorized, malicious access to TOE-controlled processing resources or information, via an unsophisticated, technical attack.
T.RECORD-EVENT	Security relevant events controlled by the TOE may not be recorded, and hence malicious activity may not be detected.
T.RESOURCES	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.
T.ROLE-SEPARATION	The development and assignment of user roles may be done in a manner that undermines security, for example assigning users conflicting roles with respect to separation of duties.
T.TOE-CORRUPTED	The security state of the TOE, as a result of an unsophisticated technical attack, may be intentionally corrupted to enable future insecurities.
T.TRACEABLE	Security relevant events controlled by the TOE may not be traceable to the user or system process/processes associated with the event.

Table 3.4.2 – Threats addressed solely by the Operational Environment

Name	Threat
T.E.ADMIN-ERROR	Authenticated users or external threat agents may, through accidental discovery or directed search, discover errors or omissions inadequacies in the security administration of the TOE, or other IT, which permit them to gain unauthorized access.
T.E.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.
T.E.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.
T.E.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.
T.E.INSTALL	The system may be delivered or installed in a manner that undermines security.
T.E.MALWARE	The confidentiality, integrity or availability of assets may be compromised as a result of the execution of malware (e.g. viruses, worms, Trojans, and so on).

Note that there may be additional threats to be countered by other (non-TOE) IT within the operational environment of the TOE. Such IT components (and their relation to the TOE) will be described in the TOE Overview section of the Security Target for the conformant TOE, and the threats they are required to counter will be specified in its security problem definition.

4. SECURITY OBJECTIVES

4.1 TOE SECURITY OBJECTIVES

Table 4.1 specifies the security objectives to be met by CCOPP-OS conformant TOEs.

Table 4.1 – TOE Security Objectives

TOE Security Objective	Security Problem Addressed
O.ACCOUNTABILITY: The TOE must ensure, for actions under its control or knowledge, that all TOE users can subsequently be held accountable for their security relevant actions.	T.TRACEABLE T.RECORD-EVENT P.ACCOUNTABILITY P.USAGE
O.AUDITING: The TOE must record security relevant events in sufficient detail to help an administrator detect attempted security violations or potential misconfiguration of security functions that would leave IT assets at risk of compromise. The TOE must present this information to authorized administrators, and ensure that its confidentiality and integrity are protected.	T.RECORD-EVENT
O.AVAILABLE: The TOE must protect itself from unsophisticated, denial-of-service attacks. This will include a combination of protection and detection.	T.DENIAL
O.BYPASS: The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement.	All threats in Table 3.4.1.
O.DETECT: The TOE must enable the detection of TOE specific insecurities.	T.TOE-CORRUPTED
O.DISCRETIONARY-ACCESS: The TOE must control access to resources/objects based on identity of users. The TOE must allow authorized users to specify which resources may be accessed by which users.	T.ACCESS P.ACCESS P.NEED-TO-KNOW
O.DUTY: The TOE must provide the capability of enforcing 'separation of duties', so that no single user has to be granted the right to perform all operations on important information.	T.ROLE-SEPARATION
O.ENFORCEMENT: The TOE must be designed and implemented in a manner which ensures that the organizational policies are enforced in the target environment.	All threats in Table 3.4.1
O.ENTRY: The TOE must prevent logical entry to the TOE by persons or processes without authority for such access, using unsophisticated technical methods.	T.ENTRY P.AUTHORIZED-USER P.USAGE
O.HIERARCHICAL: The TOE must allow hierarchical definitions of roles to facilitate administration of the TOE, i.e. the ability to define roles in terms of other roles.	T.ROLE-SEPARATION

TOE Security Objective	Security Problem Addressed
O.MANAGE: The TOE must provide all the functions and facilities necessary to support the authorized administrators, ensuring that only authorized administrators can access such functionality.	All threats in Table 3.4.1
O.MANDATORY-ACCESS: The TOE must control access to resources based upon the compartment based access restriction rules for the information being accessed and the compartment of the subject.	T.ACCESS P.ACCESS P.COMPARTMENT P.NEED-TO-KNOW
O.RECOVER: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of insecurity.	T.CRASH T.TOE-CORRUPTED
O.RESOURCES: The TOE must protect itself from user or system errors that result in shared resource exhaustion.	T.RESOURCES
O.RESIDUAL-INFORMATION: The TOE must ensure that any information contained in a protected resource is never revealed when the resource is reused by a different subject.	T.ACCESS P.ACCESS P.NEED-TO-KNOW
O.ROLE: The TOE must prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations.	T.ACCESS T.ROLE-SEPARATION P.ACCESS P.NEED-TO-KNOW

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The purpose of the environmental objectives is to state what is expected of the TOE's environment in terms of risk mitigation or explicit risk acceptance.

Table 4.2 – Security Objectives for the Operational Environment

Environmental Security Objective	Security Problem Addressed
O.E.AUDIT-MANAGE: Those responsible for the TOE must ensure that audit data is analyzed on a regular basis, that audit logs are backed up and retained for subsequent analysis where needed, and that appropriate measures are taken to guard against loss of audit data.	T.RECORD-EVENT T.TRACEABLE P.ACCOUNTABLE
O.E.AUTHENTICATION: The IT environment must provide one or more additional authentication mechanisms that can be used by the TOE when making authentication decisions.	T.ENTRY
O.E.CONNECT: Those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of the assets it is intended to protect.	A.PEER

Environmental Security Objective	Security Problem Addressed
O.E.CREDEN: Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner which maintains the security of the assets it is intended to protect.	T.ENTRY
O.E.DENIAL-SOPHISTICATED: The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks, with a focus on detection and response.	T.E.DENIAL-SOPHISTICATED
O.E.DETECT-SOPHISTICATED: The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state).	T.TOE-CORRUPTED
O.E.ENTRY-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by other than authenticated users. The focus will be on prevention, with user awareness playing a major part.	T.E.ENTRY-NON-TECHNICAL
O.E.ENTRY-SOPHISTICATED: The TOE environment must sufficiently mitigate the threat of an individual (other than an authenticated user) gaining unauthorized access via sophisticated, technical attack, with a focus on detection and response.	T.E.ENTRY-SOPHISTICATED
O.E.INSTALL: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains the security of the assets it is intended to protect.	T.E.INSTALL T.E.ADMIN-ERROR All threats in Table 3.4.1
O.E.MALWARE: Those responsible for the TOE must ensure that the risk of introduction of malware is mitigated by the deployment of appropriate countermeasures (IT and procedural).	T.E.MALWARE
O.E.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.	A.LOCATE A.PROTECT
O.E.SECURITY-ATTRIBUTES: Those responsible for the TOE must establish and implement procedures to ensure that security attributes (e.g. subject compartment labels, access rights, roles) are correctly determined and applied.	A.ACCESS A.COMPARTMENT T.E.ADMIN-ERROR All threats in Table 3.4.1
O.E.TRUSTED-ADMIN: Those responsible for the TOE must implement procedures to ensure that adequate trust is established in the TOE administrators, that they are made aware of their responsibilities for security, and that they are given appropriate training so as to effectively discharge those responsibilities.	A.MANAGE A.NO-EVIL-ADMIN T.E.ADMIN-ERROR P.TRAINING
O.E.USER-AWARENESS: Those responsible for the TOE must implement procedures to ensure that adequate trust is established in the TOE users, that they are made aware of their responsibilities for security, and that they are given appropriate training so as to effectively discharge those responsibilities.	A.ACCESS A.COOP A.USER-NEED A.USER-TRUST P.TRAINING

5. SECURITY FUNCTIONAL REQUIREMENTS

This chapter contains the specification of the Security Functional Requirements (SFRs) that must be satisfied by the CCOPP-OS conformant TOE. These are listed in Table 5.1 below.

Most of these SFRs have been specified using functional components taken from CC Part 2. All extended functional components are identified by inclusion of 'CCOPP' in the reference label (e.g. FDP_RIP.CCOPP). The definition for all such extended functional components (including dependencies) is provided in Chapter 9.

Table 5.1 – TOE Security Functional Requirements

Section	CC Component	Auditable event
5.1	**FAU**	
5.1.1	FAU_GEN.1 Audit data Generation	Start-up and shutdown of the audit functions
5.1.2	FAU_GEN.2 User Identity Generation	None
5.1.3	FAU_SAR.1 Audit Review	Reading of information from audit records
5.1.4	FAU_SAR.2 Restricted Audit Review	Unsuccessful attempts to read information from the audit records
5.1.5	FAU_SAR.3 Selectable Audit Review	None
5.1.6	FAU_SEL.1 Selective Audit	All modifications to the audit configuration that occur while the audit collection functions are operating
5.1.7	FAU_STG.1 Protected audit trail storage	None
5.1.8	FAU_STG.3 Action in case of Possible Audit Data Loss	Actions taken due to exceeding of a threshold
5.1.9	FAU_STG.4 Prevention of audit data loss	Actions taken due to the audit storage failure
5.2	**FDP**	
5.2.1	FDP_ACC.1-A Discretionary Access Control Policy	None
5.2.2	FDP_ACF.1-A Discretionary Access Control Policy Rules	All requests to perform an operation on an object covered by the SFP
5.2.3	FDP_ACC.1-B Role-Based Access Control Policy	None

Section	CC Component	Auditable event
5.2.4	FDP_ACF.1-B Role-Based Access Control Policy Rules	All requests to perform an operation on an object covered by the SFP
5.2.5	FDP_ETC.1 Export Of User Data	All attempts to export information
5.2.6	FDP_IFC.1 Mandatory Access Control Policy	None
5.2.7	FDP_IFF.1 Mandatory Access Control Policy Rules	All requests to perform an operation on an object covered by the SFP
5.2.8	FDP_ITC.1 Import Of User Data	All attempts to import user data, including any security attributes
5.2.9	FDP_RIP.2 Object Residual Information Protection	None
5.2.10	FDP_RIP.CCOPP Subject Residual Information Protection	None
5.3	**FIA**	
5.3.1	FIA_AFL.1 Authentication Failure Handling	Actions taken when the threshold is reached
5.3.2	FIA_ATD.1 User Attribute Definition	None
5.3.3	FIA_SOS.1 Verification of Passwords	Rejection or acceptance by the TSF of any tested secret
5.3.4	FIA_UAU.2 User Authentication Before Any Action	All use of the authentication mechanism
5.3.5	FIA_UAU.CCOPP Multiple Authentication Mechanisms Support	None
5.3.6	FIA_UAU.6 Re-authentication	All use of the authentication mechanism
5.3.7	FIA_UAU.7 Protected Authentication Feedback	None
5.3.8	FIA_UID.2 User Identification Before Any Action	All use of the authentication mechanism, including the identity provided during *successful* attempts.
5.3.9	FIA_USB.1 User-Subject Binding	Success and failure of binding user security attributes to a subject (e.g. success and failure to create a subject).

Section	CC Component	Auditable event
5.4	**FMT**	
5.4.1	FMT_MSA.1-A Management Of DAC Object Security Attributes	All modifications of the values of security attributes
5.4.2	FMT_MSA.1-B Management Of RBAC Object Security Attributes	All modifications of the values of security attributes
5.4.3	FMT_MSA.1-C Management Of MAC Object Security Attributes	All modifications of the values of security attributes
5.4.4	FMT_MSA.1-D Management Of User Security Attributes	All modifications of the values of security attributes
5.4.5	FMT_MSA.2 Secure RBAC Attributes	All offered and rejected values for a security attribute
5.4.6	FMT_MSA.3-A DAC Static attribute initialization	Modifications of the default settings of permissive or restrictive rules. All modifications of the initial value of security attribute.
5.4.7	FMT_MSA.3-B RBAC Static attribute initialization	Modifications of the default settings of permissive or restrictive rules. All modifications of the initial value of security attribute.
5.4.8	FMT_MSA.3-C MAC Static attribute initialization	Modifications of the default settings of permissive or restrictive rules. All modifications of the initial value of security attribute.
5.4.9	FMT_MTD.1-A Management of Audit Trail	All modifications to the Audit Trail.
5.4.10	FMT_MTD.1-B Management of Audited Events	All modifications to the subset of audited events.
5.4.11	FMT_MTD.1-C Management of Authentication Data – Initialization	All initial assignments of authentication data
5.4.12	FMT_MTD.1-D Management of Authentication Data – Modification	All modifications to the values of the authentication data
5.4.13	FMT_MTD.1-E Management of TOE Access Banner	All modifications to TOE Access Banner
5.4.14	FMT_MTD.1-F Management of Role Definitions	All modifications to Role Definitions
5.4.15	FMT_MTD.3 Secure Role Definitions	All rejected values of Role Definitions

Section	CC Component	Auditable event
5.4.16	FMT_REV.1-A Revocation of User Attributes	All attempts to revoke user attributes
5.4.17	FMT_REV.1-B Revocation of Object Attributes	All attempts to revoke object attributes
5.4.18	FMT_SAE.1 Time-Limited Authorization	All attempts to change limits
5.4.19	FMT_SMF.1 Specification of management functions	Use of the management functions
5.4.20	FMT_SMR.2 Security Roles	Every use of the rights of a role
5.5	**FPT**	
5.5.1	FPT_FLS.1 Failure with preservation of secure state	Failure of the TSF.
5.5.2	FPT_ITC.CCOPP Inter-TSF Confidentiality During Transmission	None
5.5.3	FPT_ITI.CCOPP Inter-TSF detection of modification	None
5.5.4	FPT_RCV.1 Manual recovery	The fact that a failure or service discontinuity occurred. Resumption of the regular operation. Type of failure or service discontinuity.
5.5.5	FPT_RCV.4 Function recovery	If possible, the impossibility to return to a secure state after a failure of the TSF. If possible, the detection of a failure of a function.
5.5.6	FPT_STM.1 Reliable Time Stamps	Changes to the time
5.5.7	FPT_TEE.1 Testing of External Entities	Execution of the tests of the underlying machine and the results of the tests.
5.5.8	FPT_TST.1 TSF Testing	Execution of the TSF self tests and the results of the tests.
5.6	**FRU**	
5.6.1	FRU_PRS.1 Limited Priority of Service	Rejection of operation based on the use of priority within an allocation.
5.6.2	FRU_RSA.1 Maximum quotas	Rejection of allocation operation due to resource limits.

Section	CC Component	Auditable event
5.7	**FTA**	
5.7.1	FTA_LSA.1 Limitation on scope of selectable attributes	All attempts at selecting a session security attribute.
5.7.2	FTA_MCS.1 Basic limitation on multiple concurrent session	Rejection of a new session based on the limitation of multiple concurrent sessions.
5.7.3	FTA_SSL.4 User-initiated termination	Termination of an interactive session by the user.
5.7.4	FTA_TAB.1 Default TOE access banners	None
5.7.5	FTA_TAH.1 TOE access history	None
5.7.6	FTA_TSE.1 TOE session establishment	All attempts at establishment of a user session.

The following conventions are used in the specification of the SFRs to highlight where an operation is performed on a CC Part 2 component:

- *Italicized text* is used to highlight where a selection or assignment operation has been completed in the PP.
- **Emboldened text** is used to highlight where the refinement operation has been applied, where this results in modification or insertion (though not, obviously, deletion) or words from the original CC Part 2 text (excluding wording within an open assignment or selection: see below for the treatment of this special case.)
- A letter ("-A", "-B", "-C", and so on) is appended to the CC Part 2 component or element label to indicate use of the iteration operation, where the different iterations are distinguished by sequential lettering.

Additionally, the following conventions are used in the SFR specifications:

- Underlining of <u>assignment</u> or <u>selection</u> indicates the use of a refined but uncompleted assignment or selection operation, as appropriate. This technique is used where it is appropriate to direct the ST author into completing the operation in a particular manner. For example, a selection operation may be refined by excluding one or more of the options presented in CC Part 2. Note that when a refined operation is completed, the resultant SFR will comply with the relevant CC Part 2 component, but in such a way as to be consistent with the CCOPP-OS objectives.
- In some cases it has been necessary to use extended functional components, based on existing CC Part 2 components. "CCOPP" is used in the SFR label to denote such an extended component.

5.1 AUDIT (FAU)

5.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1: The TSF shall be able to generate an audit record of the *auditable events listed in column "Auditable Event" of Table 5.1 (TOE Security Functional Requirements).*

CCOPP-OS Application Note: Table 5.1 includes all auditable events for the *basic* level of audit - except for the need to record the user identity during failures associated with FIA_UID.1 - for all SFRs taken from the CAPP and the RBAC PP. The selection operation in FAU_GEN.1.1b) has thus been completed by choosing the "Not Specified" level of audit; this has been omitted from the SFR specification for the sake of clarity and readability.

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 (if applicable), and the outcome (success or failure) of the event;
b) *The role that made possible the invocation of the action;*
c) *The compartment labels of subjects; and*
d) *The additional information specified in the "Auditable Events" column of Table 5.1.*

CCOPP-OS Application Note: For some situations it is possible that some events cannot be automatically generated. This is usually due to the audit functions not being operational at the time these events occur. Such events need to be documented in the Operational Guidance, along with recommendation on how manual auditing should be established to cover these events.

5.1.2 User Identity Generation (FAU_GEN.2)

FAU_GEN.2.1: For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.3 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: The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

CCOPP-OS Application Note: The minimum information which must be provided is the same that which is required to be recorded in 5.1.1. The intent of this requirement is that there exist tools for administrators to be able to access the audit trail in order to analyze it. Exactly what manner is provided is an implementation decision, but it needs to be done in a way which allows the administrator to make effective use of the information presented. This requirement is closely tied to 5.1.5 and 5.1.6. It is expected that a single tool will exist within the TSF which will satisfy all of these requirements.

5.1.4 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.

CCOPP-OS Application Note: By default, authorized administrators may be considered to have been granted read access to the audit records. The TSF may provide a mechanism which allows other users to also read audit records.

5.1.5 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1: The TSF shall provide the ability to apply *selection and ordering* of audit data based on the following attributes:

  a) *User identity;*
  b) *Object identity and type of access (where applicable);*
  c) *Role that enabled invocation of the action;*
  d) *Subject compartment label;*
  e) *Date and time of audit event;*
  f) *[assignment: list of additional attributes that audit selectivity is based upon].*

CCOPP-OS Application Note: The ST must state the additional attributes that audit selectivity may be based upon (e.g., type of event, success/failure), if any.

5.1.6 Selective Audit (FAU_SEL.1)

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

  a) *User identity;*
  b) *Users belonging to a specified role and access types (e.g. delete, insert) on a particular object;*
  c) *Subject identity;*
  d) *Object identity;*
  e) *Host identity;*
  f) *Event type;*
  g) *Subject compartment label;*
  h) *[assignment: list of additional attributes that audit selectivity is based upon].*

CCOPP-OS Application Note: The ST should state the additional attributes that audit selectivity may be based upon (e.g., success/failure), if any. The *subject identity* may be (for example) a process ID assigned by the TOE.

5.1.7 Protected Audit Trail Storage (FAU_STG.1)

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

FAU_STG.1.2: The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

CCOPP-OS Application Note: On many systems, in order to reduce the performance impact of audit generation, audit records will be temporarily buffered in memory before they are written to disk. In these cases, it is possible that some of these records will be lost if the operation of the TOE is interrupted by hardware or power failures. The developer needs to document what the likely loss will be and show that it has been minimized.

5.1.8 Action in Case of Possible Audit Data Loss (FAU_STG.3)

FAU_STG.3.1: The TSF shall *generate an alarm to the authorized administrator* if the audit trail exceeds [assignment: *an authorized administrator selectable, pre-defined limit*].

Refinement: The second assignment has been refined with respect to CC Part 2.

CCOPP-OS Application Note: For this component, an "alarm" is to be interpreted as any clear indication to the administrator that the pre-defined limit has been exceeded. The ST author must state the pre-defined limit that triggers generation of the alarm. The limit can be stated as an absolute value, or as a value that represents a percentage of audit trail capacity (e.g., audit trail 75% full). If the limit is adjustable by the authorized administrator, the ST should also incorporate an FMT requirement to manage this function.

5.1.9 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1: The TSF shall *prevent audited events, except those taken by the authorized administrator* and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

CCOPP-OS Application Note: A CCOPP-OS conformant TOE may be configurable, permitting an administrator to specify other actions to be taken if the audit trail is full. However in this event the TOE must provide the specified functionality in its evaluated configuration, and the ST should incorporate FMT_MOF.1 to restrict the ability to change the behavior of the audit function.

5.2 USER DATA PROTECTION (FDP)

5.2.1 Discretionary Access Control Policy (FDP_ACC.1-A)

FDP_ACC.1.1-A: The TSF shall enforce the *Discretionary Access Control (DAC) Policy* on [assignment: *list of subjects*] *acting on the behalf of users*, [assignment: *list of named objects*] and *all operations among subjects and objects covered by the DAC policy*.

CCOPP-OS Application Note: For most TOEs there is only one type of subject, usually called a process or task, which needs to be specified in the ST.

Any object that meets the criterion for a *named object* (see the Glossary, section 1.5) but is not controlled by the DAC policy must be justified.

The list of operations covers all operations between the above two lists. It may consist of a sublist for each subject-named object pair. Each operation needs to specify which type of access right is needed to perform the operation; for example read access or write access.

5.2.2 Discretionary Access Control Policy Rules (FDP_ACF.1-A)

FDP_ACF.1.1-A: The TSF shall enforce the *Discretionary Access Control (DAC) Policy* to objects based on the following:

a) *The user identity and group membership(s) associated with a subject; and*
b) *The following access control attributes associated with an object:*
[assignment: List of access control attributes. The attributes must provide permission attributes with:
    i) *the ability to associate allowed or denied operations with one or more user identities;*
    ii) *the ability to associate allowed or denied operations with one or more group identities; and*
    iii) *defaults for allowed or denied operations.]*

FDP_ACF.1.2-A: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*assignment*: *a set of rules specifying the Discretionary Access Control policy, where:*
i) *For each operation there shall be a rule, or rules, that use the permission attributes where the user identity of the subject matches a user identity specified in the access control attributes of the object;*
ii) *For each operation there shall be a rule, or rules, that use the permission attributes where the group membership of the subject matches a group identity specified in the access control attributes of the object; and*
iii) *For each operation there shall be a rule, or rules, that use the default permission attributes specified in the access control attributes of the object when neither a user identity nor group identity matches.*]

FDP_ACF.1.3-A: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, which explicitly authorize access of subjects to objects*].

FDP_ACF.1.4-A: The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, which explicitly deny access of subjects to objects*].

CCOPP-OS Application Note: A CCOPP-OS conformant TOE is required to implement a DAC policy, but the rules which govern the policy may vary between TOEs; those rules need to be specified in the ST. In completing the rule assignment above, the resulting mechanism must be able to specify access rules which apply to at least any single user. This single user may have a special status such as the owner of the object. The mechanism must also support specifying access to the membership of at least any single group. Conformant implementations include self/group/public controls and access control lists.

A DAC policy may cover rules on accessing public objects; i.e., objects which are readable to all authorized users, but which can only be altered by the TSF or authorized administrators.

A DAC policy may include exceptions to the basic policy for access by authorized administrators or other forms of special authorization (e.g. based on specific roles).

The ST must list the attributes which are used by the DAC policy for access decisions. These attributes may include permission bits, access control lists, and object ownership. A single set of access control attributes may be associated with multiple objects, such as all objects stored on a single floppy disk. The association may also be indirectly bound to the object, such as access control attributes being associated with the name of the object rather than directly to the object itself.

FDP_ACF.1.3-A and FDP_ACF.1.4-A should be used to define any 'exceptions' or 'overriding' of the normal DAC policy rules, in particular where any RBAC or MAC policy rules take precedence over DAC (for example, where a role has the privilege to bypass or override DAC).

5.2.3   Role-Based Access Control Policy (FDP_ACC.1-B)

FDP_ACC.1.1-B: The TSF shall enforce the *Role-Based Access Control (RBAC) Policy* on [assignment: *list of subjects*] *acting on the behalf of users*, [assignment: *list of named objects*] and *all operations among subjects and objects covered by the RBAC policy*.

CCOPP-OS Application Note: For most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST.

5.2.4   Role-Based Access Control Policy Rules (FDP_ACF.1-B)

FDP_ACF.1.1-B: The TSF shall enforce the *Role-Based Access Control (RBAC) Policy* to objects based on the following:

  a) *User identity and authorized roles for the user; and*
  b) *Subject identity and role(s) which can invoke the subject; and*
  c) *Object identity and operations permitted on the objects for the different roles.*

FDP_ACF.1.2-B: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *The subject invoking the operation on an object is assigned to a role whose privilege set includes the operation on the object.*

FDP_ACF.1.3-B: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, which explicitly authorize access of subjects to objects*].

FDP_ACF.1.4-B: The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, which explicitly deny access of subjects to objects*].

CCOPP-OS Application Note: FDP_ACF.1.3-B and FDP_ACF.1.4-B should be used to define any 'exceptions' or 'overriding' of the normal RBAC policy rules, in particular where any DAC or MAC policy rules take precedence over RBAC.

5.2.5   Export of User Data (FDP_ETC.1)

FDP_ETC.1.1: The TSF shall enforce the *Mandatory Access Control Policy* when exporting user data, controlled under the **MAC policy**, outside of the TOE, **by enforcing the following rules: [assignment:** *exportation control rules***].**

FDP_ETC.1.2: The TSF shall export the user data without the user data's associated security attributes.

Refinement: As indicated in the text of FDP_ETC.1.1, the SFR is refined to permit the specification of rules that apply to the export of user data (cf. FDP_ETC.1.3 as specified in LSPP).

CCOPP-OS Application Note: A CCOPP-OS conformant TOE must provide protections to data exported outside the control of the TOE via any communications mechanisms that do not provide security attributes along with the actual data. The device, or mechanism, used to export information must, itself, have security attributes that correspond to those of the information being exported. The ability to export information must be allowed under the existing rules that establish the MAC policy of the TOE.

The ST author must also explicitly state the rules under which authorized users can designate the security attributes of the mechanisms, or devices, used to export data without security attributes.

Single-level Input/Output devices and single-level communication channels are not required to maintain the compartment label-based access restrictions of the information they process.

If the conformant TOE implements rules governing the export of security attributes associated with other security policies (e.g. DAC) then these should be specified in the ST either by means of an appropriate iteration of FDP_ETC.1 or by the inclusion of FDP_ETC.2.

5.2.6   Mandatory Access Control Policy (FDP_IFC.1)

FDP_IFC.1.1**:**   The TSF shall enforce the *Mandatory Access Control (MAC) Policy* on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the MAC policy*].

CCOPP-OS Application Note: For most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST.

5.2.7   Mandatory Access Control Policy Rules (FDP_IFF.1)

FDP_IFF.1.1**:** The TSF shall enforce the *Mandatory Access Control (MAC) Policy* based on the following types of subject and information security attributes:

   a) *The subject compartment label; and*

b) *The compartment label of the object containing the information.*

CCOPP-OS Application Note: The compartmental label of the subject is a single non-hierarchical category. A CCOPP-OS conformant TOE may allow a subject to have multiple labels simultaneously. The compartment label of the object may be a 'conceptual label', for example taking the form of access rules that dictate how subjects in each compartment may access the object.

FDP_IFF.1.2**:** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the label-based relationship that must hold between subject and object labels*].

FDP_IFF.1.3**:** The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4: The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *rules, based on security attributes that explicitly authorize information flows*].

FDP_IFF.1.5: The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes that explicitly deny information flows*].

CCOPP-OS Application Note: FDP_IFF.1.4 and FDP_IFF.1.5 should be used to define any 'exceptions' or 'overriding' of the normal MAC policy rules, in particular where any RBAC or DAC policy rules take precedence over MAC.

5.2.8   Import of User Data (FDP_ITC.1)

FDP_ITC.1.1: The TSF shall enforce the *Mandatory Access Control Policy* when importing user data, controlled under the **MAC policy**, from outside of the TOE.

FDP_ITC.1.2: The TSF shall ignore the security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3: The TSF shall enforce the following rules when importing user data controlled under the **MAC policy** from outside the TOE: [assignment: *additional importation control rules*].

Refinement: For clarity, the generic CC term 'SFP' has been replaced with the more meaningful 'MAC policy' in FDP_ITC.1.1 and FDP_ITC.1.3.

CCOPP-OS Application Note: The CCOPP-OS conformant TOE must provide protection for data imported from outside the control of the TOE via functions that do not provide reliable security attributes along with the actual data. The imported data must be assigned compartment label-based access restriction rules that will be used to enforce the MAC policy. Further, the ability for a subject to import information must be controlled under the existing rules that establish the MAC policy of the TOE.

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.

If the conformant TOE implements rules governing the import of security attributes associated with other security policies (e.g. DAC) then these should be specified in the ST either by means of an appropriate iteration of FDP_ITC.1 or by the inclusion of FDP_ITC.2.

5.2.9 Object Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1: The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

CCOPP-OS 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. Clearing the information content of resources on de-allocation from objects is sufficient to satisfy this requirement, if unallocated resources will not accumulate new information until they are allocated again.

5.2.10 Subject Residual Information Protection (FDP_RIP.CCOPP)

FDP_RIP.CCOPP.1: The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all subjects.

CCOPP-OS 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. Clearing the information content of resources on de-allocation from subjects is sufficient to satisfy this requirement, if unallocated resources will not accumulate new information until they are allocated again.

5.3 IDENTIFICATION AND AUTHENTICATION (FIA)

5.3.1 Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1: The TSF shall detect when [selection: *[assignment: positive integer number]*, *an authorized administrator configurable positive integer within [assignment: range of acceptable values]]* unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

5.3.2   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) *User Identifier;*
   b) *Group Memberships;*
   c) *Authentication Data;*
   d) *Compartment Labels;*
   e) *User Roles;*
   f) *Default Active Role Set; and*
   g) *[assignment: other user security attributes].*

CCOPP-OS Application Note: The specified attributes are those that are required by the TSF to enforce the DAC, RBAC and MAC policies, the generation of audit records, and proper identification and authentication of users. The user identity must be uniquely associated with a single individual user.

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.

A TOE may have two forms of user and group identities, a text form and a numeric form. In these cases there must be unique mapping between the representations.

5.3.3   Verification of Authentication Data (FIA_SOS.1)

FIA_SOS.1.1: 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 1,000,000;*
   b) *For multiple attempts to use the authentication mechanism during a one minute period, the probability that a random attempt during that minute will succeed is less than one in 100,000; and*
   c) *Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics;*
   d) *[assignment: other criteria that user-generated authentication data shall meet].*

CCOPP-OS Application Note: The method of authentication is not specified by the CCOPP-OS, but must be specified in a ST. The method which is used must be shown to have low probability that authentication data can be forged or guessed. For example, if a password mechanism is used a set of metrics needs to be specified and may include such things as minimum length of the password, maximum lifetime of a password, and the subjecting of possible passwords to dictionary attacks.

5.3.4   User Authentication Before Any Action (FIA_UAU.2)

FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

CCOPP-OS Application Note: FIA_UAU.2 effectively precludes anonymous access to the TOE, unless the conformant ST can show (in its TOE Summary Specification) that such access does not count as a "TSF-mediated action", such that this might present a potential bypass attack vector against the Identification and Authentication mechanism.

5.3.5   Support for Multiple Authentication Mechanisms (FIA_UAU.CCOPP)

FIA_UAU.CCOPP.1:   The TSF shall provide support for [assignment**:** *the required use of authentication mechanisms other than only passwords, based upon access parameters such as time of day, port of entry, and user privilege*] to support user authentication.

FIA_UAU.CCOPP.2:   The TSF shall authenticate any user's claimed identity according to the [assignment**:** *parameters for selecting authenticators required, these parameters are to be specifiable by an explicitly specified set of users, enforcing least privilege on the basis of the following: [selection: explicitly authorized administrators, administrator roles, both]*].

CCOPP-OS Application Note: The ST rationale should provide a basic justification for the selection made, indicating how it supports enforcement of least privilege. Note that this SFR implies a dependency on the IT environment, which is reflected in the security objective O.E.AUTHENTICATION. If the TOE implements these additional authentication mechanisms, then the ST author should use FIA_UAU.5 instead, tailored in a way that is demonstrably consistent with FIA_UAU.CCOPP.

5.3.6   Re-authentication (FIA_UAU.6)

FIA_UAU.6.1: The TSF shall re-authenticate the user under the conditions *request to change authentication secrets, and the following additional conditions: [assignment: list of ST specific conditions under which re-authentication is required].*

CCOPP-OS Application Note: The ST rationale should provide a basic justification for the assignment made, including a "null" list, showing why it is complete.

5.3.7   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.

CCOPP-OS Application Note: Obscured feedback implies the TSF does not produce a visible display of any authentication data entered by a user, such as through a keyboard (e.g., echo the password on the workstation). It is acceptable that some indication of progress be returned instead, such as an asterisk returned for each character sent.

5.3.8   User Identification Before Any Action (FIA_UID.2)

FIA_UID.2.1: The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

CCOPP-OS Application Note: FIA_UID.2 effectively precludes anonymous access to the TOE, unless the conformant ST can show (in its TOE Summary Specification) that such access

does not count as a "TSF-mediated action", such that this might present a potential bypass attack vector against the Identification and Authentication mechanism.

5.3.9   User-Subject Binding (FIA_USB.1)

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

   a) *The user identity which is associated with auditable events;*
   b) *The user identity or identities which are used to enforce the Discretionary Access Control Policy*
   c) *The group membership or memberships used to enforce the Discretionary Access Control Policy,*
   d) *The compartment labels used to enforce the Mandatory Access Control Policy;*
   e) *The roles used to enforce the Role-Based Access Control Policy;*
   f) *[assignment: additional security attributes].*

CCOPP-OS Application Note: The DAC policy and audit generation require that each subject acting on the behalf of users have a user identity associated with the subject. This identity is normally 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 on a user identity which differs from the one used during identification. The ST must state, in FIA_USB.1.2, how this alternate identity is associated with a subject and justify why the individual user associated with this alternate identity is not compromised by the mechanism used to implement it.

"None" is a valid completion of the assignment. In this case the list item f) may be omitted for clarity.

FIA_USB.1.2:   The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

   a) *The subject user identity associated with auditable events is set to the corresponding user identity;*
   b) *The real and effective subject user identity or identities which are used to enforce the Discretionary Access Control Policy is set to the corresponding user identity or identities;*
   c) *The real and effective group identities used to enforce the Discretionary Access Control Policy are set to the user's group membership;*
   d) *The subject compartment labels are set to the user compartment labels.*
   e) *[assignment: additional rules].*

CCOPP-OS Application Note: "None" is a valid completion of the assignment. In this case the list item e) may be omitted for clarity.

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

   a) *Only authorized administrators shall be able to change the user identity and group memberships of a subject acting on his or her behalf to that of another valid user;*

b) *A subject's effective user identity is changed to the owner of a file executed with its set-user-identity permission bit enabled;*
c) *A subject's effective group identity is changed to the owning group of a file executed with its set-group-identity permission bit enabled;*
d) *[assignment: rules for the changing of compartment labels of subjects, if the TOE permits these to be set dynamically];*
e) *[assignment: additional rules].*

CCOPP-OS Application Note: If the TOE provides no capability to change the effective user identity as per rule a) then this should be stated in the ST in place of rule a). Such a TOE will still conform to the CCOPP-OS, because it is more restrictive than the PP.

If the TOE allows the current label or role to be set dynamically, the rules governing such changes must be specified here. Null assignments are permitted if no such capability is implemented.

"None" is a valid completion of the assignments at list items d) and e). In this case the list items may be omitted for clarity.

5.4   SECURITY MANAGEMENT (FMT)

5.4.1   Management of DAC Object Security Attributes (FMT_MSA.1-A)

FMT_MSA.1.1-A: The TSF shall enforce the *Discretionary Access Control Policy* to restrict the ability to *modify* the *DAC attributes associated with a named object* to [assignment: *the authorized users*].

5.4.2   Management of RBAC Object Security Attributes (FMT_MSA.1-B)

FMT_MSA.1.1-B: The TSF shall enforce the *Role-Based Access Control Policy* to restrict the ability to *modify* the *RBAC attributes associated with a named object* to *the object owner and [assignment: the authorized identified RBAC administrative roles].*

5.4.3   Management of Object Label-Based Access Restriction Rules (FMT_MSA.1-C)

FMT_MSA.1.1-C: The TSF shall enforce the *Mandatory Access Control Policy* to restrict the ability to *modify* the *compartment label-based access restriction rules associated with an object* to [assignment: *the authorized identified roles*].

CCOPP-OS Application Note: The ST must state the components of the access rights that may be modified, and must state any restrictions that may exist for a type of authorized user and the components of the access rights that the user is allowed to modify.

The ability to modify access rights must be restricted in that a user having access rights to a named object does not have the ability to modify those access rights unless granted the right to do so. This restriction may be explicit, based on the object ownership, or based on a set of object rules.

5.4.4 Management of User Security Attributes (FMT_MSA.1-D)

FMT_MSA.1.1-D: The TSF shall enforce the *Discretionary, Role-Based and Mandatory Access Control Policies* to restrict the ability to *initialize and modify* the *user security attributes, other than authentication data*, to *authorized administrators*.

CCOPP-OS Application Note: This component only applies to security attributes which are used to maintain the TSP. Other user attributes may be specified in the ST, but control of those attributes is not within the scope of the CCOPP-OS. Note that the management of authentication data is addressed by FMT_MTD.1-C and FMT_MTD.1-D below.

5.4.5 Secure RBAC Security Attributes (FMT_MSA.2)

FMT_MSA.2: The TSF shall ensure that only secure values are accepted for *RBAC security attributes and [assignment: other security attributes]*.

CCOPP-OS Application Note: The open assignment may be completed with 'none'. For the sake of readability, this completion may be indicated by deletion of the word 'and' in the text of the SFR.

5.4.6 DAC Static Attribute Initialization (FMT_MSA.3-A)

FMT_MSA.3.1-A: The TSF shall enforce the *Discretionary Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the **Discretionary Access Control Policy**.

FMT_MSA.3.2-A: The TSF shall allow the [assignment: *authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Refinement: For clarity, the generic CC term 'SFP' has been replaced with the more meaningful 'Discretionary Access Control Policy' in FMT_MSA.3.1-A.

5.4.7 RBAC Static Attribute Initialization (FMT_MSA.3-B)

FMT_MSA.3.1-B: The TSF shall enforce the *Role-Based Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the **Role-Based Access Control Policy**.

FMT_MSA.3.2-B: The TSF shall allow the [assignment: *authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Refinement: For clarity, the generic CC term 'SFP' has been replaced with the more meaningful 'Role-Based Access Control Policy' in FMT_MSA.3.1-B.

5.4.8 MAC Static Attribute Initialization (FMT_MSA.3-C)

FMT_MSA.3.1-C: The TSF shall enforce the *Mandatory Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the **Mandatory Access Control Policy**.

FMT_MSA.3.2-C: The TSF shall allow the [assignment: *authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

CCOPP-OS Application Note: A CCOPP-OS conformant TOE must provide protection by default for all objects at creation time. This may be done through the enforcing of a restrictive default access control on newly created objects or by requiring the user to explicitly specify the desired access controls on the object at its creation. In either case, there shall be no window of vulnerability through which unauthorized access may be gained to newly created objects.

Refinement: For clarity, the generic CC term 'SFP' has been replaced with the more meaningful 'Mandatory Access Control Policy' in FMT_MSA.3.1-C.

5.4.9 Management of Audit Trail (FMT_MTD.1-A)

FMT_MTD.1.1-A: The TSF shall restrict the ability to *create, delete, and clear* the *audit trail* to *authorized administrators*.

CCOPP-OS Application Note: The selection of "create, delete, and clear" functions for audit trail management reflects common management functions. These functions should be considered generic; any other audit administration functions that are critical to the management of a particular audit mechanism implementation should be specified in the ST.

5.4.10 Management of Audited Events (FMT_MTD.1-B)

FMT_MTD.1.1-B: The TSF shall restrict the ability to *modify or observe* the *set of audited events* to *authorized administrators*.

CCOPP-OS Application Note: The set of audited events are the subset of auditable events which will be audited by the TSF. The term 'set' is used loosely here and refers to the total collection of possible ways to control which audit records get generated; this could be by type of record, identity of user, identity of object, etc.

It is an important aspect of audit that users are not able to affect which of their actions are audited, and therefore must not have control over or knowledge of the selection of an event for auditing.

5.4.11 Management of Authentication Data – Initialization (FMT_MTD.1-C)

FMT_MTD.1.1-C: The TSF shall restrict the ability to *initialize* the *authentication data* to *authorized administrators*.

5.4.12 Management of Authentication Data – Modification (FMT_MTD.1-D)

FMT_MTD.1.1-D: The TSF shall restrict the ability to *modify* the *authentication data* to *the following:*

  a) *authorized administrators; and*
  b) *users authorized to modify their own authentication data.*

CCOPP-OS Application Note: User authentication data refers to information that users must provide to authenticate themselves to the TSF. Examples include passwords, personal identification numbers, and fingerprint profiles. User authentication data does not include the user's identity. The ST must specify the authentication mechanism that makes use of the user authentication data to verify a user's identity.

This component does not require that users be authorized to modify their own authentication information; it only states that it is permissible.

5.4.13 Management of TOE Access Banner (FMT_MTD.1-E)

FMT_MTD.1.1-E: The TSF shall restrict the ability to *modify* the *TOE Access Banner* to *authorized administrators*.

5.4.14 Management of Role Definitions (FMT_MTD.1-F)

FMT_MTD.1.1-F: The TSF shall restrict the ability to *create and modify* the *Role Definitions, Role Attributes, Role Hierarchies, and Constraints among Role Relationships* to *authorized administrators*.

5.4.15 Secure Role Definition Values (FMT_MTD.3)

FMT_MTD.3.1: The TSF shall ensure that only secure values are accepted for *Role Definitions, Role Attributes, Role Hierarchies and Constraints among Role Relationships, [assignment: other security attributes]*.

CCOPP-OS Application Note: The open assignment may be completed with 'none'. For the sake of readability, this completion may be indicated by deletion of the word 'and' in the text of the SFR.

5.4.16 Revocation of User Security Attributes (FMT_REV.1-A)

FMT_REV.1.1-A: The TSF shall restrict the ability to revoke *all security attributes* associated with the *users* under the control of the TSF to *authorized administrators*.

FMT_REV.1.2-A: The TSF shall enforce the rules:

a) *The immediate revocation of user security attributes; and*
b) *[assignment: list of other revocation rules concerning users].*

CCOPP-OS Application Note: Many user security attributes could have serious consequences if misused, so an immediate revocation method must exist, although it need not be the usual method (e.g., the usual method may be editing the trusted user's profile, but the change doesn't take effect until the user logs off and logs back on. The method for immediate revocation might be to edit the trusted user's profile and "force" the trusted user to log off.). The immediate method must be specified in the ST and in administrator guidance. In a distributed environment the developer must provide a description of how the "immediate" aspect of this requirement is met.

5.4.17 Revocation of Object Security Attributes (FMT_REV.1-B)

FMT_REV.1.1-B: The TSF shall restrict the ability to revoke *all security attributes* associated with *objects* under the control of the TSF to *users authorized to modify the security attributes by the Discretionary, Role-Based or Mandatory Access Control policies*.

FMT_REV.1.2-B: The TSF shall enforce the rules:

 a) *The access rights associated with an object shall be enforced when an access check is made;*
 b) *The rules of the Mandatory Access Control policy are enforced on all future operations; and*
 c) *[assignment: list of other revocation rules concerning objects]*.

CCOPP-OS Application Note: The DAC policy may include immediate revocation (e.g. Multics immediately revokes access to segments) or delayed revocation (e.g., most UNIX systems do not revoke access to already opened files). The DAC access rights are considered to have been revoked when all subsequent access control decisions by the TSF use the new access control information. It is not required that every operation on an object make an explicit access control decision as long as a previous access control decision was made to permit that operation. It is sufficient that the developer clearly documents in guidance documentation how revocation is enforced.

5.4.18 Time-Limited Authorization (FMT_SAE.1)

FMT_SAE.1.1: The TSF shall restrict the capability to specify an expiration time for *user account and authenticators and [assignment: list of additional security attributes for which expiration is to be supported]* to *the authorized administrator*.

FMT_SAE.1.2: For each of these security attributes, TSF shall be able to *for user account – disable account and require administrator action to re-enable, for authenticators – require owner of authenticator to establish a new value before proceeding with authenticated action and [assignment: list of additional actions to be taken for each security attribute]* after the expiration time for the indicated security attribute has passed.

CCOPP-OS Application Note: The ST rationale shall provide a basic justification for the assignment made, to include a "null" assignment, showing that it is a complete list with respect to the attributes which must be restricted to enforce secure operation.

The ST rationale should also provide a basic justification for the selection made in FMT_SAE.1.1, indicating how it enforces least privilege.

The ST rationale should provide a basic justification for the assignment made in FMT_SAE.1.2, to include "null", showing that it is sufficient to enable secure operation.

5.4.19 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

   a) *Management of Object Security Attributes;*
   b) *Management of User Security Attributes;*
   c) *Management of Authentication Data;*
   d) *Management of Audit Trail;*
   e) *Management of Auditable Events;*
   f) *Management of TOE Access Banner;*
   g) *Management of Role Definitions, including Role Hierarchies and Constraints;*
   h) *[assignment: additional security management functions].*

CCOPP-OS Application Note: The assignment at list item h) should be completed to list any additional security management functions that are desired, or which are implied by other FMT SFRs that are included in the ST but not in the CCOPP-OS. If no such claims are needed this list item may be omitted (in effect, completing the assignment with "none").

5.4.20 Security Roles (FMT_SMR.2)

FMT_SMR.2.1: The TSF shall maintain the roles:

   a) *authorized administrator;*
   b) *object owners;*
   c) *users authorized by the Discretionary Access Control Policy to modify object security attributes;*
   d) *users authorized by the Mandatory Access Control Policy to modify object security attributes;*
   e) *users authorized to modify their own authentication data; and*
   f) *[assignment: other roles as needed to enforce the RBAC policy].*

FMT_SMR.2.2: The TSF shall be able to associate users with roles.

FMT_SMR.2.3: The TSF shall ensure that the **following** conditions *for (a) Roles of Object Owners and (b) the set of RBAC administrative roles* are satisfied:

   a) *Object Owners can modify security attributes for only the objects they own;*
   b) *The set of RBAC administrative roles can modify security attributes for all objects under the control of TOE (since they automatically inherit the privileges of all Object Owners).*

CCOPP-OS Application Note: A CCOPP-OS-conformant TOE only needs to support a single administrative role, referred to as the authorized administrator. If a TOE implements multiple independent roles, the ST should refine the use of the term authorized administrators to specify which roles fulfill which requirements.

The CCOPP-OS specifies a number of functions which are required of or restricted to an authorized administrator, but there may be additional functions which are specific to the TOE. This would include any additional function which would undermine the proper operation of the TSF. Examples of functions include: ability to access certain system resources like tape drives or

vector processors, ability to manipulate the printer queues, and the ability to run real-time programs.

5.5 PROTECTION OF TOE SECURITY FUNCTIONS (FPT)

5.5.1 Failure With Preservation of Secure State (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

a) *The entire RBAC database containing data on privileges assigned to a role, users authorized for a role, role constraints and relationships, or some specific tables containing subsets of these data are off-line, corrupt or inaccessible.*

b) *[assignment: list of other TSF failures for which the ST is able to preserve a secure state].*

CCOPP-OS Application Note: As the purpose of this requirement is to make the list of recoverable failures explicit, not to mandate specific failures (other than those needed for RBAC PP conformance), the ST rationale does not need to show completeness. However, the ST rationale does need to provide a basic justification for the claim that the ST will preserve a secure state for each failure type listed.

5.5.2 Subset Inter-TSF Confidentiality During Transmission (FPT_ITC.CCOPP)

FPT_ITC.CCOPP.1: The TSF shall support the protection of *authentication information* transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

CCOPP-OS Application Note: This and the following SFR refer to the communication of authentication data between the TOE and add-on packages that provide additional authentication mechanisms (as indicated in O.E.AUTHENTICATION and FIA_UAU.CCOPP). Note that if there is a need to detail the specific protection measures employed (e.g. TLS, SSL, IPsec) this can be done in the ST either through refinement of the above SFR, or in the TOE Summary Specification description of how the SFR is met.

Should the conformant TOE itself provide those additional mechanisms (and hence implements FIA_UAU.5) then this requirement can be satisfied by FPT_ITT.1, FPT_ITT.2 or a suitably extended component, tailored in a way that provides demonstrably equivalent protection of authentication data transmitted on internal channels. If the TOE implementation is such that FIA_UAU.5 is met *without* any transmission of authentication data between separate parts of the TOE, then this SFR can be argued as being trivially met.

5.5.3 Subset Inter-TSF detection of modification (FPT_ITI.CCOPP)

FPT_ITI.CCOPP.1: The TSF shall support the capability to verify the integrity of *authentication information* transmitted between the TSF and another trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

CCOPP-OS Application Note: The ST rationale shall provide a basic justification, showing that the ST assignment is complete.

Should the conformant TOE itself provide additional authentication mechanisms (and hence implements FIA_UAU.5) then this requirement can be satisfied by FPT_ITT.1, FPT_ITT.2 or a suitably extended component tailored in a way that provides demonstrably equivalent protection of authentication data transmitted on internal channels. If the TOE implementation is such that FIA_UAU.5 is met *without* any transmission of authentication data between separate parts of the TOE, then this SFR can be argued as being trivially met.

Refinement: See text in FPT_ITI.CCOPP.1.

5.5.4   Manual Recovery (FPT_RCV.1)

FPT_RCV.1.1:   After [assignment: *list of types of TSF failures*], the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

5.5.5   Function Recovery (FPT_RCV.4)

FPT_RCV.4.1: The TSF shall ensure that *the following functions and failure scenarios* have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state:

   a) *For the function that checks whether a specified privilege is assigned to any role: a failure scenario where the database containing the privilege data is not on-line or the particular data table is inaccessible or corrupt.*
   b) *For the function that checks whether a specified role has been assigned to a particular user: a failure scenario where the database containing the role membership information is not on-line or the particular data table is inaccessible or corrupt.*
   c) *[assignment: list of other function and failure scenarios].*

5.5.6   Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1: The TSF shall be able to provide reliable time stamps.

CCOPP-OS Application Note: The generation of audit records depends on having a correct date and time. The ST needs to specify the degree of accuracy that must be maintained in order to maintain useful information for audit records.

5.5.7   Testing of External Entities (FPT_TEE.1)

FPT_TEE.1.1: The TSF shall run a suite of tests *periodically during normal operation, at the request of an authorized administrator, [selection: "during initial start-up," [assignment: other conditions]]* to check the fulfillment of *the security assumptions provided by the abstract machine that underlies the TSF*.

FPT_TEE.1.2: If the test fails, the TSF shall [assignment: *action(s)*].

CCOPP-OS Application Note: In general this component refers to the proper operation of the hardware platform on which a TOE is running. The test suite needs to cover only aspects of the hardware on which the TSF relies to implement required functions, including domain separation. If a failure of some aspect of the hardware would not result in the TSF compromising the functions it performs, then testing of that aspect is not required. Note that the selection operation permits a null choice, i.e. allows the ST author to specify whether or not the tests are run during initial start-up.

5.5.8 TSF Testing (FPT_TST.1)

FPT_TST.1.1: The TSF shall run a suite of self tests *periodically during normal operation, at the request of the authorized user, and when invocation of access rights on [assignment: selected objects] occurs* to demonstrate the correct operation of the TSF.

FPT_TST.1.2: The TSF shall provide authorized users with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3: The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

CCOPP-OS Application Note: The ST should identify the role(s) that are allowed to execute the self tests.

5.6 RESOURCE UTILIZATION (FRU)

5.6.1 Limited Priority of Service (FRU_PRS.1)

FRU_PRS.1.1: The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2: The TSF shall ensure that each access to [assignment: *controlled resources*] shall be mediated on the basis of the subject's assigned priority.

5.6.2 Maximum Quotas (FRU_RSA.1)

FRU_RSA.1.1: The TSF shall enforce maximum quotas of the following resources: [assignment: *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

CCOPP-OS Application Note: The ST rationale must show that the list of resources for which maximum quotas is enforced is sufficiently complete to accomplish protection against resource exhaustion, to the extent that the OS is capable of doing so. Also the ST rationale must give, for both selections, the reasoning for the choices made and stating why the choices support the goal of protecting against denial-of-service.

5.7 TOE ACCESS (FTA)

5.7.1 Limitation on Scope of Selectable Attributes (FTA_LSA.1)

FTA_LSA.1.1 The TSF shall restrict the scope of **these** session security attributes: *user role, user compartment label, and [assignment: list of other session security attributes]*, based on [selection: *point of entry, time of day, day of week, [assignment: list of other attributes]*].

CCOPP-OS Application Note: This SFR calls for the TOE to have the *capability* of restricting the scope of the listed session security attributes, i.e. that it will enforce the restrictions if configured to do so. The ST rationale should provide a basic justification, showing that the ST specific assignments are sufficient to restrict the security critical attributes.

Refinement: See text in FTA_LSA.1.1.

5.7.2 Basic Limitation on Multiple Concurrent Sessions (FTA_MCS.1)

FTA_MCS.1.1: The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2: The TSF shall enforce, by default, a limit of [assignment**:** *default number*] sessions per user.

5.7.3 User-Initiated Termination (FTA_SSL.4)

FTA_SSL.4.1: The TSF shall allow user-initiated user-termination of the user's own interactive session.

CCOPP-OS Application Note: In some environments the requirement FTA_SSL.2 may also be needed to allow greater user flexibility, e.g. where other measures such as physical access controls cannot be relied upon to prevent unauthorized access to an unattended session. In such environments FTA_SSL.2 should also be included in the ST.

5.7.4 Default TOE Access Banners (FTA_TAB.1)

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

5.7.5 TOE access history (FTA_TAH.1)

FTA_TAH.1.1: Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last successful session establishment to the user.

FTA_TAH.1.2: Upon successful session establishment, the TSF shall display the [selection**:** *date, time, method, 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: The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

5.7.6 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1: The TSF shall be able to deny session establishment based on *the Default Active Role Set for the user being empty and [assignment: additional security attributes]*.

CCOPP-OS Application Note: In the context of this (RBAC PP) requirement, the term 'session' does not necessarily mean a regular login session (such that login is denied if the user has no assigned roles): it is permissible for the TOE to implement the notion of a session *within* a regular login session, during which one or more authorized user roles may be activated for a user. In this case, FTA_TSE.1 requires that establishment of such a session shall be denied if a user has no authorized roles. Any such interpretations must be described in the TOE Summary Specification of the ST, showing how FTA_TSE.1 is met by the TOE.

It is acceptable for 'none' to be chosen for the assignment; in this case the nugatory word 'and' may be deleted for the sake of readability.

6. ASSURANCE REQUIREMENTS

The assurance requirements for CCOPP-OS are met by EAL4. EAL4 stresses assurance through vendor actions that are within the bounds of current best-commercial-practice. EAL4 provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL4 also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented; (3) verification of a sample of the vendor functional testing; (4) searching for obvious vulnerabilities; and (5) independent functional testing.

The assurance components for EAL4 are summarized in Table 6.1.

Table 6.1 – EAL4 Assurance Components

Assurance Class	Assurance Components
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent Testing – Sample
Class AVA: Vulnerability Assessment	AVA_VAN.3 Focused Vulnerability analysis

7. RATIONALE

This chapter provides the rationale for the security objectives and requirements specified in this PP. Section 7.1 provides the rationale for the security objectives based upon their suitability to address the security problem definition. Section 7.2 provides the rationale for the security requirements, demonstrating their suitability to achieve the stated security objectives for the TOE.

7.1 SECURITY OBJECTIVES RATIONALE

7.1.1 Complete Coverage – Environmental Assumptions

This section provides evidence demonstrating that the security objectives for the operational environment uphold the environmental assumptions. The following table shows the assumption to objective mapping.

Table 7.1 Security Objectives to Environment Assumptions

Assumption	Security Objectives	Upholds Assumption By:
A.COMPARTMENT	O.E.SECURITY-ATTRIBUTES	Ensuring that security attributes (including compartmental labels) are correctly determined and applied.
A.PEER	O.E.CONNECT	Ensuring that external connections do not undermine security.
A.LOCATE	O.E.PHYSICAL	Ensuring that the TOE hardware and software is physically protected.
A.PROTECT	O.E.PHYSICAL	Ensuring that the TOE hardware and software is physically protected.
A.ACCESS	O.E.SECURITY-ATTRIBUTES	Ensuring that security attributes, including roles, are properly determined and assigned.
	O.E.TRUSTED-ADMIN	Ensuring that adequate trust is established in administrators and that they are made aware of their security responsibilities, so that they do not abuse their roles.
	O.E.USER-AWARENESS	Ensuring that adequate trust is established in users and that they are made aware of their security responsibilities, so that they do not abuse their roles.
A.COOP	O.E.USER-AWARENESS	Ensuring that users are made aware of their responsibilities and that adequate trust is established in them

Assumption	Security Objectives	Upholds Assumption By:
A.MANAGE	O.E.TRUSTED-ADMIN	Ensuring that appropriate individuals are assigned to administrator roles.
A.NO-EVIL-ADMIN	O.E.TRUSTED-ADMIN	Ensuring that adequate trust is established in those assigned to administrator roles.
A.USER-NEED	O.E.USER-AWARENESS	Ensuring that users are made aware of their responsibilities
A.USER-TRUST	O.E.USER-AWARENESS	Ensuring that procedures are in place to establish trust in users

7.1.2   Complete Coverage – Threats

Table 7.2 Threats to Security Objectives

Threat	Security Objectives	Helps Counter Threat By:
T.ACCESS	O.DISCRETIONARY-ACCESS	Controlling access to resources or information based on user identity
	O.MANDATORY-ACCESS	Controlling access to resources based on subject compartment labels
	O.RESIDUAL-INFORMATION	Preventing bypass of access controls through access to residual information
	O.ROLE	Controlling access based on roles
T.CRASH	O.RECOVER	Providing for recovery to a secure state in the event of a system crash.
T.DENIAL	O.AVAILABLE	Ensuring the TOE protects itself from unsophisticated denial of service attacks.
T.ENTRY	O.ENTRY	Ensuring that only identified and authenticated users can gain logical entry to the TOE.
	O.E.CREDEN	Ensuring that unauthorized logical entry to the TOE is prevented user authentication data is appropriately protected within the environment.
	O.E.AUTHENTICATION	Providing additional authentication mechanisms to strengthen the TOE authentication where appropriate.
T.RECORD-EVENT	O.ACCOUNTABILITY	Ensuring that TOE users can be held accountable for their security relevant actions.
	O.AUDITING	Ensuring that security relevant events are recorded.

Threat	Security Objectives	Helps Counter Threat By:
	O.E.AUDIT-MANAGE	Ensuring that the audit trail is analyzed and managed to prevent loss of data.
T.RESOURCES	O.RESOURCES	Ensuring the TOE protects itself against resource exhaustion errors (user or system generated).
T.ROLE-SEPARATION	O.DUTY	Ensuring that the TOE has the capability of enforcing separation of duty.
	O.HIERARCHICAL	Enabling the definition of role hierarchies to facilitate role administration.
	O.ROLE	Controlling access based on roles.
T.TOE-CORRUPTED	O.DETECT	Ensuring that the TOE can detect insecurities arising from low grade attacks.
	O.RECOVER	Ensuring that the TOE can recover to a secure state following detection of insecurity.
	O.E.DETECT-SOPHISTICATED	Providing for supporting environmental measures to detect sophisticated attack not covered by O.DETECT.
T.TRACEABLE	O.ACCOUNTABILITY	Ensuring that TOE users are accountable for their security relevant actions.
	O.E.AUDIT-MANAGE	Ensuring that the audit trail is analyzed and managed to prevent loss of data.
All	O.BYPASS	Ensuring that the TOE security functions cannot be bypassed
	O.ENFORCEMENT	Ensuring that the TOE security functions are invoked and operate correctly.
	O.MANAGE	Ensuring that the TOE security functions are underpinned by appropriate security management functionality.
	O.E.INSTALL	Ensuring secure delivery, installation, management and operation of the TOE.
	O.E.SECURITY-ATTRIBUTES	Ensuring that associated security attributes are properly determined and applied.

Threat	Security Objectives	Helps Counter Threat By:
T.E.ADMIN-ERROR	O.E.INSTALL	Ensuring that the TOE is installed and operated in a way that maintains security.
	O.E.SECURITY-ATTRIBUTES	Ensuring that security attributes are properly applied.
	O.E.TRUSTED-ADMIN	Ensuring that administrators are properly trained and aware of their responsibilities, thus minimizing the risk of administrator error through incompetence or carelessness.
T.E.DENIAL-SOPHISTICATED	O.E.DENIAL-SOPHISTICATED	Self-evident.
T.E.ENTRY-NON-TECHNICAL	O.E.ENTRY-NON-TECHNICAL	Self-evident.
T.E.ENTRY-SOPHISTICATED	O.E.ENTRY-SOPHISTICATED	Self-evident.
T.E.INSTALL	O.E.INSTALL	Self-evident.
T.E.MALWARE	O.E.MALWARE	Self-evident.

7.1.3 Complete Coverage – Policy

This section provides evidence demonstrating coverage of the Organizational Security Policy by both the TOE and environmental security objectives. The following table shows this objective to policy mapping, and the table is followed by a discussion of the coverage for each Security Policy.

Table 7.3 Organizational Security Policies to Security Objectives

OSP	Security Objectives	Upholds OSP By:
P.ACCESS	O.DISCRETIONARY-ACCESS	Controlling access to resources or information based on user identity
	O.MANDATORY-ACCESS	Controlling access to resources based on subject compartment labels
	O.RESIDUAL-INFORMATION	Preventing bypass of access controls through access to residual information
	O.ROLE	Controlling access based on roles
P.ACCOUNTABILITY	O.ACCOUNTABILITY	Self-evident.
P.AUTHORIZED-USER	O.ENTRY	Preventing unauthorized logical entry to the TOE.
P.COMPARTMENT	O.MANDATORY-ACCESS	Enforcing a MAC policy based on subject compartment labels.
P.NEED-TO-KNOW	O.DISCRETIONARY-ACCESS	Controlling access to resources or information based on user identity
	O.MANDATORY-ACCESS	Controlling access to resources based on subject compartment labels

OSP	Security Objectives	Upholds OSP By:
	O.RESIDUAL-INFORMATION	Preventing compromise of need-to-know through access to residual information
	O.ROLE	Controlling access based on roles
P.TRAINING	O.E.TRUSTED-ADMIN	Ensuring that administrators are given appropriate training
	O.E.USER-AWARENESS	Ensuring that users are given appropriate training
P.USAGE	O.ENTRY	Preventing logical entry to the TOE by unauthorized users.
	O.ACCOUNTABILITY	Deterring unauthorized usage by authorized users, ensuring they are accountable for their actions.

7.2 SECURITY REQUIREMENTS RATIONALE

This PP as a whole provides evidence supporting the combined internal consistency and completeness of the functional components that comprise the PP against the CAPP and RBAC. Although there is no Rationale Section within the RBAC, the Rationale for [CAPP] plus the additional information provided in this section plus other tables accomplishes the requirements.

7.2.1 Security Requirements cover Security Objectives

The following table demonstrates that the IT security requirements are suitable to achieve the TOE security objectives. For the most part, this rationale focuses on the SFRs, as the SARs play a supporting role in achieving the TOE security objectives. One exception is ADV_ARC.1, which addresses the non-bypassability and domain separation requirements that were considered to be SFRs in earlier versions of the CC.

It will also be noted that the rationale for O.AVAILABLE is more general than that given for other TOE security objectives. This reflects the nature of the security objective: there are many SFRs that help achieve the objective, but none that are included in the PP that have the *specific* aim of defending the TOE against low-grade denial of service attacks.

Table 7.4 TOE Security Objectives to Security Requirements

Security Objective	Requirement	Helps Achieve Objective By:
O.ACCOUNTABILITY	FAU_GEN.1	Recording security relevant events caused by users
	FAU_GEN.2	Ensuring that the identity of the user responsible for the event is recorded where relevant.
	FIA_USB.1	Ensuring that the user identity is associated with subjects created to act on behalf of that user.
O.AUDITING	FAU_GEN.1	Recording security relevant events caused by users

Security Objective	Requirement	Helps Achieve Objective By:
	FAU_GEN.2	Recording the identity of users responsible for security relevant events
	FAU_SAR.1	Enabling administrators to review generated audit data
	FAU_SAR.2	Protecting the confidentiality of audit data
	FAU_SAR.3	Providing administrators with the tools necessary to analyze audit data
	FAU_SEL.1	Enabling administrators to manage the audit configuration according to the specific needs of the environment.
	FAU_STG.1	Protecting the integrity of the audit trail
	FAU_STG.3	Helping to guard against potential loss of audit data
	FAU_STG.4	Helping to guard against potential loss of audit data
	FMT_MTD.1-A	Preventing unauthorized modification of the audit trail
	FMT_MTD.1-B	Ensuring that only authorized administrators can manage the audit configuration.
	FPT_STM.1	Providing trusted timestamps in support of auditing.
O.AVAILABLE	FIA SFRs FTA SFRs	Preventing logical entry to the TOE by unauthorized personnel who might otherwise exploit this to cause denial of service to other users.
	FDP SFRs FMT SFRs	Controlling the ability of authorized users to access data or perform operations that might cause denial of service to other users.
	FAU SFRs	Helping to detect security relevant events that might be indicative of a denial of service attack.
	FRU SFRs	Preventing excessive consumption of resources by authorized users that might cause denial of service to other users.
	FPT_RCV.1 FPT_RCV.4	Providing trusted recovery to a secure state in the event of detected failures, thus mitigating against the effects of a denial of service attack.
O.BYPASS	ADV_ARC.1	Ensuring the TOE security architecture prevents bypass of the TOE security functions.
	FDP_RIP.2	Preventing bypass of access controls through access to residual information.
	FDP_RIP.CCOPP	Preventing bypass of access controls through access to residual information.
	FPT_ITC.CCOPP FPT_ITI.CCOPP	Prevents bypass of TOE security functions arising from access to TSF data when in transit between different parts of a distributed TOE.

Security Objective	Requirement	Helps Achieve Objective By:
O.DETECT	FAU_GEN.1	Recording security relevant events to enable detection of TOE insecurities.
	FAU_SAR.1	Providing the ability to review audit information to help detect TOE insecurities.
	FAU_SAR.3	Providing an audit analysis capability to enable detection of TOE insecurities.
	FAU_SEL.1	Providing the capability to manage the audit trail to help better detect TOE insecurities.
	FAU_STG.1 FAU_STG.3 FAU_STG.4 FMT_MTD.1-A FMT_MTD.1-B	Protecting the integrity and availability of generated audit data.
	FIA_AFL.1	Detecting and responding to repeated authentication failures.
	FMT_TEE.1	Detecting potential TOE insecurities owing to errors in the operation of the underlying abstract machine.
	FPT_TST.1	Detecting possible compromise of the integrity of TSF data or TOE executable files.
	FTA_TAH.1	Helping users to detect possible unauthorized login attempts against their user account.
O.DISCRETIONARY_ACCESS	FDP_ACC.1-A	Defining the scope of the DAC policy.
	FDP_ACF.1-A	Enforcing the DAC policy rules.
	FIA_ATD.1 FIA_USB.1	Maintaining user security attributes necessary for DAC enforcement, and applying them appropriately to subjects created to act on a user's behalf.
	FMT_MSA.1-A FMT_MSA.1-D FMT_MSA.3-A	Providing secure management (including initialization) of DAC object and user security attributes.
	FMT_REV.1-A FMT_REV.1-B	Providing the ability to revoke user and object security attributes used to enforce the DAC policy.
O.DUTY	FMT_SMR.2	Providing for separation of roles.
O.ENFORCEMENT	ADV_ARC.1	Ensuring that the TOE security architecture provides for a secure initialization process and prevents tampering with the TOE security functions.
	FPT_TEE.1	Helping ensure the correct operation of the underlying abstract machine in support of the TOE security functions.
	FPT_FLS.1	Ensuring that the TOE preserves a secure state for specified failures.

Security Objective	Requirement	Helps Achieve Objective By:
	FPT_ITC.CCOPP FPT_ITI.CCOPP	Ensuring that TSF data is protected, enabling continued enforcement of the TOE security functions, when in transit between different parts of a distributed TOE.
	FPT_TST.1	Helping to ensure continued enforcement of the TOE security functions by detecting loss of integrity in TSF data or TSF executables.
O.ENTRY	FIA_UID.2	Preventing unauthorized logical entry by ensuring a valid user identity is entered.
	FIA_UAU.2	Preventing unauthorized logical entry by ensuring a valid user password is entered.
	FIA_AFL.1	Preventing repeated failed authentication attempts to guard against unauthorized logical entry.
	FIA_SOS.1	Strengthening the quality of entered authentication data.
	FIA_UAU.CCOPP	Providing support for multiple authentication mechanisms to strengthen authentication of users.
	FIA_UAU.6	Preventing unauthorized logical entry by requiring re-authentication of users at suitable points.
	FIA_UAU.7	Guarding against password entry being observed by unauthorized personnel.
	FMT_MTD.1-C FMT_MTD.1-D	Providing secure management (including initialization) of authentication data.
	FTA_TAB.1 FMT_MTD.1-E	Providing a TOE access banner with a configurable advisory warning message to deter unauthorized logical access.
	FMT_SAE.1 FPT_STM.1	Strengthening authentication by enforcing regular password change, and providing trusted timestamps in support of this.
	FPT_ITC.CCOPP FPT_ITI.CCOPP	Protecting TSF data in transit between different parts of a distributed TOE, thereby preventing unauthorized logical entry being gained by this route.
	FTA_LSA.1 FTA_TSE.1	Controlling entry to the TOE on the basis of role attributes, thus supporting the achievement of this objective.
	FTA_MCS.1	Limiting the number of multiple concurrent sessions for a user, which helps to reduce the likelihood of successful unauthorized logical entry whilst the relevant user is already logged in elsewhere.
	FTA_SSL.4	Preventing unauthorized logical entry via an unattended user session.

Security Objective	Requirement	Helps Achieve Objective By:
	FTA_TAB.1	Displaying an advisory warning message to deter unauthorized logical entry
	FTA_TAH.1	Helping to guard against unauthorized logical entry by providing the means for users to detect such attempts against their account.
O.HIERARCHICAL	FMT_SMF.1	Providing the ability to define role hierarchies
	FMT_MTD.1-F	Restricting the ability to define role hierarchies to authorized administrators.
O.MANAGE	FAU_SAR.1 FAU_SAR.3	Providing authorized administrators with the capability to review and analyze audit data.
	FAU_SEL.1	Providing the ability to manage the audit configuration.
	FAU_STG.3 FAU_STG.4	Providing authorized administrators with management functionality to help prevent audit data loss.
	FMT_MSA.1-A FMT_MSA.1-B FMT_MSA.1-C FMT_MSA.1-D FMT_MSA.3-A FMT_MSA.3-B FMT_MSA.3-C	Providing the ability to manage object and user security attributes.
	FMT_MSA.2	Supporting management of role attributes by ensuring only secure values are provided.
	FMT_MTD.1-E	Providing the ability to manage the TOE access banner (advisory warning message).
	FMT_REV.1-A FMT_REV.1-B	Providing the ability to revoke user and object security attributes.
	FMT_SAE.1	Providing the ability to manage password expiry limits.
	FMT_SMF.1	Providing the required security management functions.
	FMT_SMR.2	Supporting security management by maintaining roles.
O.MANDATORY_ACCESS	FDP_IFC.1	Defining the scope of the MAC policy.
	FDP_IFF.1	Enforcing the MAC policy rules
	FDP_ETC.1	Enforcing the MAC policy on export of user data.
	FDP_ITC.1	Enforcing the MAC policy on import of user data.
	FIA_ATD.1 FIA_USB.1	Maintaining user security attributes necessary for MAC enforcement, and applying them appropriately to subjects created to act on a user's behalf.

Security Objective	Requirement	Helps Achieve Objective By:
	FMT_MSA.1-C FMT_MSA.1-D FMT_MSA.3-C	Providing secure management (including initialization) of MAC object and user security attributes.
	FMT_REV.1-A FMT_REV.1-B	Providing the ability to revoke user and object security attributes used to enforce the MAC policy.
O.RECOVER	FPT_RCV.1	Ensuring that the TOE recovers to a secure state following specified TSF failures, by manual means.
	FPT_RCV.4	Ensuring that the TOE recovers to a secure state in the event of specific failures of security functions.
O.RESOURCES	FRU_PRS.1	Mitigating against excessive use of resources by low priority activities by ensuring that high priority activities.
	FRU_RSA.1	Controlling the consumption of resources by imposing quotas on resource usage.
	FTA_MCS.1	Controlling the consumption of resources by limiting the number of multiple concurrent sessions for users.
O.RESIDUAL_INFORMATION	FDP_RIP.2	Providing residual information protection when objects are reused.
	FDP_RIP.CCOPP	Providing residual information protection when subjects are reused.
O.ROLE	FDP_ACC.1-B	Defining the scope of the RBAC policy.
	FDP_ACF.1-B	Enforcing the RBAC policy rules
	FIA_ATD.1 FIA_USB.1	Maintaining user security attributes necessary for RBAC enforcement, and applying them appropriately to subjects created to act on a user's behalf.
	FMT_MSA.1-B FMT_MSA.1-D FMT_MSA.3-B	Providing secure management (including initialization) of RBAC object and user security attributes.
	FMT_MSA.2	Supporting management of role attributes by ensuring only secure values are provided.
	FMT_MTD.1-F FMT_MTD.3	Providing for secure management of role definitions.
	FMT_REV.1-A FMT_REV.1-B	Providing the ability to revoke user and object security attributes used to enforce the RBAC policy.
	FMT_SMR.2	Maintaining the roles needed to enforce the RBAC policy.
	FTA_LSA.1 FTA_TSE.1	Supports the RBAC policy by controlling entry to the TOE on the basis of role attributes.

7.2.2 Satisfaction of Dependencies

The table below demonstrates that all dependencies amongst the TOE security functional requirements of the TOE are satisfied within this PP. (No analysis is provided for the SARs as this is a self-contained assurance package.) For each SFR, the dependency of the relevant component, as specified in CC Part 2, is listed. The table references the PP SFR that satisfies the dependency (distinguishing between different iterations where necessary).

The following points should be noted regarding the content of this table:

- "(H)" signifies that the dependency is satisfied by a component that is hierarchical to the minimum requirement.
- For each extended component, dependencies have been determined based on those that are declared in [CC] for the CC Part 2 component that it is based on, according to the Extended Components Definition (see chapter 9).

Table 7.5 Dependency Analysis for TOE SFRs

Section	SFR	Dependency from CC	Satisfied in PP by SFR in Section:
5.1.1	FAU_GEN.1	FPT_STM.1	5.5.6, FPT_STM.1
5.1.2	FAU_GEN.2	FAU_GEN.1	5.1.1, FAU_GEN.1
		FIA_UID.1	5.3.8, FIA_UID.2 (H)
5.1.3	FAU_SAR.1	FAU_GEN.1	5.1.1, FAU_GEN.1
5.1.4	FAU_SAR.2	FAU_SAR.1	5.1.3, FAU_SAR.1
5.1.5	FAU_SAR.3	FAU_SAR.1	5.1.3, FAU_SAR.1
5.1.6	FAU_SEL.1	FAU_GEN.1	5.1.1, FAU_GEN.1
		FMT_MTD.1	5.4.10, FMT_MTD.1-B
5.1.7	FAU_STG.1	FAU_GEN.1	5.1.1, FAU_GEN.1
5.1.8	FAU_STG.3	FAU_STG.1	5.1.7, FAU_STG.1
5.1.9	FAU_STG.4	FAU_STG.1	5.1.7, FAU_STG.1
5.2.1	FDP_ACC.1-A	FDP_ACF.1	5.2.2, FDP_ACF.1-A
5.2.2	FDP_ACF.1-A	FDP_ACC.1	5.2.1, FDP_ACC.1-A
		FMT_MSA.3	5.4.6, FMT_MSA.3-A
5.2.3	FDP_ACC.1-B	FDP_ACF.1	5.2.4, FDP_ACF.1-B
5.2.4	FDP_ACF.1-B	FDP_ACC.1	5.2.3, FDP_ACC.1-B
		FMT_MSA.3	5.4.7, FMT_MSA.3-B
5.2.5	FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	5.2.6, FDP_IFC.1
5.2.6	FDP_IFC.2	FDP_IFF.1	5.2.7, FDP_IFF.1
5.2.7	FDP_IFF.1	FDP_IFC.1	5.2.6, FDP_IFC.1
		FMT_MSA.3	5.4.8, FMT_MSA.3-C
5.2.8	FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	5.2.6, FDP_IFC.1
		FMT_MSA.3	5.4.8, FMT_MSA.3-C
5.2.9	FDP_RIP.2	None	N/A

Section	SFR	Dependency from CC	Satisfied in PP by SFR in Section:
5.2.10	FDP_RIP.CCOPP	None	N/A
5.3.1	FIA_AFL.1	FIA_UAU.1	5.3.4, FIA_UAU.2 (H)
5.3.2	FIA_ATD.1	None	N/A
5.3.3	FIA_SOS.1	None	N/A
5.3.4	FIA_UAU.2	FIA_UID.1	5.3.8, FIA_UID.2 (H)
5.3.5	FIA_UAU.CCOPP	None	N/A
5.3.6	FIA_UAU.6	None	N/A
5.3.7	FIA_UAU.7	FIA_UAU.1	5.3.4, FIA_UAU.2 (H)
5.3.8	FIA_UID.2	None	N/A
5.3.9	FIA_USB.1	FIA_ATD.1	5.3.2, FIA_ATD.1
5.4.1	FMT_MSA.1-A	FDP_ACC.1 or FDP_IFC.1	5.2.1, FDP_ACC.1-A
		FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.2	FMT_MSA.1-B	FDP_ACC.1 or FDP_IFC.1	5.2.3, FDP_ACC.1-B
		FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.3	FMT_MSA.1-C	FDP_ACC.1 or FDP_IFC.1	5.2.6, FDP_IFC.1
		FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.4	FMT_MSA.1-D	FDP_ACC.1 or FDP_IFC.1	5.2.1, FDP_ACC.1-A 5.2.3, FDP_ACC.1-B 5.2.6, FDP_IFC.1
		FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.5	FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1	5.2.3, FDP_ACC.1-B
		FMT_MSA.1	5.4.2, FMT_MSA.1-B
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.6	FMT_MSA.3-A	FMT_MSA.1	5.4.1, FMT_MSA.1-A
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.7	FMT_MSA.3-B	FMT_MSA.1	5.4.2, FMT_MSA.1-B
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.8	FMT_MSA.3-C	FMT_MSA.1	5.4.3, FMT_MSA.1-C
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.9	FMT_MTD.1-A	FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.10	FMT_MTD.1-B	FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.11	FMT_MTD.1-C	FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)

Section	SFR	Dependency from CC	Satisfied in PP by SFR in Section:
5.4.12	FMT_MTD.1-D	FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.13	FMT_MTD.1-E	FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.14	FMT_MTD.1-F	FMT_SMF.1	5.4.19, FMT_SMF.1
		FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.15	FMT_MTD.3	FMT_MTD.1	5.4.14, FMT_MTD.1-F
5.4.16	FMT_REV.1-1	FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.17	FMT_REV.1-2	FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
5.4.18	FMT_SAE.1	FMT_SMR.1	5.4.20, FMT_SMR.2 (H)
		FPT_STM.1	5.5.6, FPT_STM.1
5.4.19	FMT_SMF.1	None	N/A
5.4.20	FMT_SMR.2	FIA_UID.1	5.3.8, FIA_UID.2 (H)
5.5.1	FPT_FLS.1	None	N/A
5.5.2	FPT_ITC.CCOPP	None	N/A
5.5.3	FPT_ITI.CCOPP	None	N/A
5.5.4	FPT_RCV.1	AGD_OPE.1	(EAL4 requirement)
5.5.5	FPT_RCV.4	None	N/A
5.5.6	FPT_STM.1	None	N/A
5.5.7	FPT_TEE.1	None	N/A
5.5.8	FPT_TST.1	None	N/A
5.6.1	FRU_PRS.1	None	N/A
5.6.2	FRU_RSA.1	None	N/A
5.7.1	FTA_LSA.1	None	N/A
5.7.2	FTA_MCS.1	FIA_UID.1	5.3.8, FIA_UID.2 (H)
5.7.3	FTA_SSL.4	None	N/A
5.7.4	FTA_TAB.1	None	N/A
5.7.5	FTA_TAH.1	None	N/A
5.7.6	FTA_TSE.1	None	N/A

7.2.3   Rationale for Assurance Level

This protection profile has been developed for a generalized environment with a moderate level of risk to the assets. It is intended that products used in these environments will be generally available, without modification to meet the security needs of the environment. As such it was determined the Evaluation Assurance Level 4 was the most appropriate.

8. CONFORMANCE CLAIM RATIONALE

This chapter provides the rationale for the conformance of the CCOPP-OS with the CAPP (Section 8.1) and RBAC PP (Section 8.2). The aim of this rationale is to demonstrate that a TOE that conforms to the CCOPP-OS will also conform to the CAPP and RBAC PPs, without the need for its ST to explicitly justify conformance to those two PPs.

8.1 CONFORMANCE TO CAPP

8.1.1 Consistency of TOE Type

Both the CAPP and CCOPP-OS are written to specify security requirements for operating systems.

8.1.2 Consistency of Security Problem Definition

Consistency is demonstrated in the following table. Note that the CAPP does not specify any threats. In several cases the rationale states that a CAPP OSP is equivalent to a CCOPP-OS threat. Equivalence in this context means that both ways of expressing this aspect of the security problem can be addressed by the same security objective(s).

CCOPP-OS does not require the TOE to counter threats based on "sophisticated technical attacks". This is consistent with [CAPP, 1.2] which states that it is appropriate for "an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security". The CAPP is not intended to be applicable to where "protection is required against determined attempts by hostile and well funded attackers to breach system security".

Table 8.1 Consistency with CAPP Security Problem Definition

CAPP Statement	CCOPP-OS Statement	Rationale
A.LOCATE	A.LOCATE	Self-evident
A.PROTECT	A.PROTECT	Self-evident
A.MANAGE	A.MANAGE	Self-evident
A.NO_EVIL_ADM	A.NO-EVIL-ADMIN	Self-evident
A.COOP	A.COOP	Self-evident
A.PEER	A.PEER	Self-evident
A.CONNECT	A.LOCATE	The CCOPP-OS assumption incorporates the CAPP assumption
P.AUTHORIZED_USERS	P.AUTHORIZED-USER T.ENTRY	Self-evident. (Note that the CAPP policy is also equivalent to the CCOPP-OS threat, i.e. they imply the same security objective(s).)

CAPP Statement	CCOPP-OS Statement	Rationale
P.NEED_TO_KNOW	P.NEED-TO-KNOW	Self-evident
P.ACCOUNTABILITY	P.ACCOUNTABILITY	Self-evident

8.1.3   Consistency of Security Objectives

Consistency is demonstrated in the following table.

Table 8.2 Consistency with CAPP Security Objectives

CAPP Statement	CCOPP-OS Statement	Rationale
O.AUTHORIZATION	O.ENTRY	Self-evident
O.DISCRETIONARY_ACCESS	O.DISCRETIONARY-ACCESS	Self-evident
O.AUDITING	O.AUDITING	Self-evident
O.RESIDUAL_INFORMATION	O.RESIDUAL-INFORMATION	Self-evident
O.MANAGE	O.MANAGE	Self-evident
O.ENFORCEMENT	O.ENFORCEMENT	Self-evident
O.INSTALL	O.E.INSTALL	Self-evident. CCOPP-OS makes explicit what is meant by 'maintains IT security objectives' in CAPP.
O.PHYSICAL	O.E.PHYSICAL	Self-evident
O.CREDEN	O.E.CREDEN	Self-evident

8.1.4   Consistency of Security Requirements

Consistency is demonstrated in the following table. Note that the CAPP does not adopt any labeling scheme for extended components, or for distinguishing between iterations of components. In these cases, the table below identifies the relevant section in CAPP to uniquely reference the SFR.

Table 8.3 Consistency with CAPP Security Functional Requirements

CAPP SFR	CCOPP-OS SFR	Rationale
FAU_GEN.1	FAU_GEN.1	The CCOPP-OS SFR includes all auditable events and information required by the CAPP.
FAU_GEN.2	FAU_GEN.2	Self-evident
FAU_SAR.1	FAU_SAR.1	Self-evident
FAU_SAR.2	FAU_SAR.2	Self-evident
FAU_SAR.3	FAU_SAR.3	The CCOPP-OS SFR includes the CAPP criteria.
FAU_SEL.1	FAU_SEL.1	The CCOPP-OS SFR includes the CAPP criteria.
FAU_STG.1	FAU_STG.1	Self-evident

CAPP SFR	CCOPP-OS SFR	Rationale
FAU_STG.3	FAU_STG.3	Self-evident
FAU_STG.4	FAU_STG.4	Self-evident
FDP_ACC.1	FDP_ACC.1-A	Self-evident
FDP_ACF.1	FDP_ACF.1-A	Self-evident
FDP_RIP.2	FDP_RIP.2	Self-evident
"Note 1" (CAPP 5.2.4)	FDP_RIP.CCOPP	Self-evident
FIA_ATD.1	FIA_ATD.1	The CCOPP-OS SFR includes all CAPP user security attributes.
FIA_SOS.1	FIA_SOS.1	The CCOPP-OS SFR includes all CAPP criteria.
FIA_UAU.1	FIA_UAU.2	The CCOPP-OS SFR is hierarchical to the CAPP SFR.
FIA_UAU.7	FIA_UAU.7	Self-evident
FIA_UID.1	FIA_UID.2	The CCOPP-OS SFR is hierarchical to the CAPP SFR.
FIA_USB.1	FIA_USB.1	The CAPP SFR was written as a refinement of the existing FIA_USB.1 component. These refinements are explicitly incorporated as assignments in CC Version 3, which the CCOPP-OS uses.
FMT_MSA.1	FMT_MSA.1-A	Self-evident
FMT_MSA.3	FMT_MSA.3-A	Self-evident
FMT_MTD.1 (5.4.3)	FMT_MTD.1-A	Self-evident
FMT_MTD.1 (5.4.4)	FMT_MTD.1-B	Self-evident
FMT_MTD.1 (5.4.5)	FMT_MSA.1-D	The requirements are equivalent (the only difference being that the CCOPP-OS SFR makes explicit mention of the policies associated with the security attributes).
FMT_MTD.1 (5.4.6.1)	FMT_MTD.1-C	Self-evident
FMT_MTD.1 (5.4.6.2)	FMT_MTD.1-D	Self-evident
FMT_REV.1 (5.4.7)	FMT_REV.1-A	Self-evident
FMT_REV.1 (5.4.8)	FMT_REV.1-A	Self-evident
FMT_SMR.1	FMT_SMR.2	The CCOPP-OS SFR is hierarchical to that mandated by the CAPP, and includes all CAPP roles.
FPT_AMT.1	FPT_TEE.1	FPT_TEE.1 is the generalized equivalent of FPT_AMT.1 at CCv3.1R2. The CCOPP-OS refines the selection operation to restrict the possible choices. As this is a valid refinement, it is consistent with CAPP (completion of the selection in a CCOPP-OS conformant ST always results in an SFR that conforms to the CAPP requirement).
FPT_RVM.1	ADV_ARC.1	At CC Version 3 the non-bypassability requirement is now covered by this EAL4 requirement.
FPT_SEP.1	ADV_ARC.1	At CC Version 3 the domain separation requirement is now covered by this EAL4 requirement.

CAPP SFR	CCOPP-OS SFR	Rationale
FPT_STM.1	FPT_STM.1	Self-evident

8.2   CONFORMANCE TO RBAC PP

8.2.1   Consistency of TOE Type

Both the RBAC PP and CCOPP-OS are written to specify security requirements for operating systems (the RBAC PP also includes other types of TOE such as database management systems and other applications within its scope).

8.2.2   Consistency of Security Problem Definition

Consistency is demonstrated in the following table. CCOPP-OS does not require the TOE to counter threats based on "sophisticated technical attacks". Whilst the RBAC PP does not explicitly rule out such attacks, the assurance level and strength of function requirements it mandates are consistent with this approach (i.e., the RBAC PP does not require protection against attackers who have a higher attack potential than those addressed by CCOPP-OS).

Table 8.4 Consistency with RBAC PP Security Problem Definition

RBAC PP Statement	CCOPP-OS Statement	Rationale
A.ASSET	A.LOCATE A.PROTECT	This assumption falls into two parts. Aspects relating to physical protection are covered by the two CCOPP-OS assumptions stated here. The statement on asset value is reflected in the description of assets in chapter 3.
A.LOCATE	A.LOCATE	Self-evident
A.PROTECT	A.PROTECT	Self-evident
A.ACCESS	A.ACCESS	Self-evident
A.MANAGE	A.MANAGE	Self-evident
A.OWNER	None	This assumption has not been included in the CCOPP-OS as the restriction it imposes is unnecessary, given the other policies enforced by the conformant TOE. The DAC policy in particular permits wider object ownership than is the case for TOEs that only implement an RBAC policy.
A.CONNECT	A.LOCATE	The RBAC assumption is included in A.LOCATE.
P.ACCESS	P.ACCESS	Self evident

RBAC PP Statement	CCOPP-OS Statement	Rationale
T.ACCESS	T.ACCESS	The CCOPP-OS threat is, in effect, and expanded version of the RBAC PP threat.
T.ENTRY	T.ENTRY	Self-evident (see the general statement above)
T.OPERATE	T.E.ADMIN-ERROR	The CCOPP-OS statement covers the threat of insecure operation.
T.ROLEDEV	T.ROLE-SEPARATION	Self-evident

8.2.3 Consistency of Security Objectives

Consistency is demonstrated in the following table.

Table 8.5 Consistency with RBAC PP Security Objectives

RBAC PP Statement	CCOPP-OS Statement	Rationale
O.ACCOUNT	O.ACCOUNTABILITY	The CCOPP-OS objective fully includes and expands slightly on the RBAC objective.
O.ADMIN	O.MANAGE	Self-evident
O.AUDIT	O.AUDITING	Self-evident
O.DUTY	O.DUTY	Self-evident
O.ENTRY	O.ENTRY	Self-evident
O.HIERARCHICAL	O.HIERARCHICAL	Self-evident
O.KNOWN	O.ENTRY	The need to reliably identify users before access rights can be granted is inherent within the CCOPP-OS objective.
O.ROLE	O.ROLE	Self-evident
O.CONNECT	O.E.CONNECT	Self-evident
O.INSTALL	O.E.INSTALL	Self-evident
O.PHYSICAL	O.E.PHYSICAL	Self-evident

8.2.4 Consistency of Security Requirements

Consistency is demonstrated in the following table.

Table 8.6 Consistency with RBAC PP Security Functional Requirements

RBAC PP SFR	CCOPP-OS SFR	Rationale
FAU_GEN.1	FAU_GEN.1	The CCOPP-OS SFR includes all auditable events and information required by the RBAC PP.
FAU_GEN.2	FAU_GEN.2	Self-evident
FAU_SAR.1	FAU_SAR.1	Self-evident
FAU_SAR.2	FAU_SAR.2	Self-evident
FAU_SAR.3	FAU_SAR.3	All RBAC PP criteria are included.
FAU_SEL.1	FAU_SEL.1	All RBAC PP criteria are included.
FAU_STG.1	FAU_STG.1	Self-evident
FDP_ACC.1	FDP_ACC.1-B	Self-evident
FDP_ACF.1	FDP_ACF.1-B	The differences in FDP_ACF.1.3 and FDP_ACF.1.4 reflect the interactions between RBAC and DAC and MAC. In the CCOPP-OS these elements have been used as intended by CC i.e. to define exceptions to the policy. The RBAC requirements in these two elements are fully addressed in FDP_ACF.1.2.
FIA_ATD.1	FIA_ATD.1	All RBAC PP user security attributes are included (note that 'user roles' is the same as 'list of authorized roles' in this context).
FIA_UAU.2	FIA_UAU.2	Self-evident
FIA_UID.2	FIA_UID.2	Self-evident
FIA_USB.1	FIA_USB.1	The CCOPP-OS SFR uses the current form of FIA_USB.1, which specifies, *inter alia*, that all appropriate RBAC attributes are applied to subjects.
FMT_MSA.1	FMT_MSA.1-B	Covers the object security attributes for RBAC
	FMT_MSA.1-D	Covers the user security attributes for RBAC
	FIA_USB.1	Covers the session Active Role Set (in FIA_USB.1.3e).
FMT_MSA.2	FMT_MSA.2	The scope of the SFR is restricted to the RBAC requirement, i.e. RBAC-specific attributes. This was necessary to avoid conflicts with other policies implemented by the CCOPP-OS conformant TOE. The SFRs are equivalent with respect to RBAC.
FMT_MSA.3	FMT_MSA.3-B	Self-evident
FMT_MTD.1	FMT_MTD.1-C FMT_MTD.1-D	Covers user passwords (a)
	FMT_MTD.1-F	Covers role definitions, hierarchies, constraints (b-d)
	FMT_MTD.1-B	Covers audited events (e)
FMT_MTD.3	FMT_MTD.3	The scope of the SFR is restricted to the RBAC requirement, i.e. RBAC-specific TSF data. This was necessary to avoid conflicts with other policies implemented by the CCOPP-OS conformant TOE. The SFRs are equivalent with respect to RBAC.

RBAC PP SFR	CCOPP-OS SFR	Rationale
FMT_REV.1	FMT_REV.1-A	Covers the user security attribute aspect
	FMT_REV.1-B	Covers the object security attribute aspect
FMT_SMR.2	FMT_SMR.2	Self-evident
FPT_AMT.1	FPT_TEE.1	FPT_TEE.1 is the generalized equivalent of FPT_AMT.1 at CCv3.1R2. The CCOPP-OS retains the flexibility of also mandating the running of diagnostic tests during initial start-up.
FPT_FLS.1	FPT_FLS.1	The RBAC PP requirement is included within the scope of the CCOPP-OS SFR as a minimum.
FPT_RCV.1	FPT_RCV.1	Self-evident
FPT_RCV.4	FPT_RCV.4	The RBAC PP requirement is included within the scope of the CCOPP-OS SFR as a minimum.
FPT_RVM.1	ADV_ARC.1	At CC Version 3 the non-bypassability requirement is now covered by this EAL4 requirement.
FPT_SEP.1	ADV_ARC.1	At CC Version 3 the domain separation requirement is now covered by this EAL4 requirement.
FPT_STM.1	FPT_STM.1	Self-evident
FPT_TST.1	FPT_TST.1	The RBAC PP requirement is included within the scope of the CCOPP-OS SFR as a minimum.
FTA_LSA.1	FTA_LSA.1	Self-evident
FTA_TSE.1	FTA_TSE.1	Self-evident

9. EXTENDED COMPONENTS DEFINITION

This chapter provides the definition of the extended components used in the specification of the SFRs in chapter 5. This is to satisfy the APE_ECD.1 criteria. The extended components are specified using the same model for structure and presentation as CC Part 2. This definition also explains why the extension is necessary, and describes the relationship to existing CC Part 2 components and families. It should be noted that dependencies for each of these components are as declared for the CC Part 2 component on which they are based.

9.1 CLASS FDP – USER DATA PROTECTION

9.1.1 Subject Residual Information Protection - FDP_RIP.CCOPP

This component was included to comply with the CAPP. It is identical to FDP_RIP.2 (and hence is considered as part of an extended FDP_RIP family), apart from the substitution of "objects" with "subjects". See the CAPP for further details.

FDP_RIP.CCOPP.1: The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, de-allocation of the resource from*] all subjects.

9.2 CLASS FIA – IDENTIFICATION AND AUTHENTICATION

9.2.1 Support for Multiple Authentication Mechanisms - FIA_UAU.CCOPP

This component is closely related to FIA_UAU.5, and hence is considered as part of an extended FIA_UAU family. It is identical in wording apart from the inclusion of the words "provide support for". This means that a conformant TOE does not need to implement multiple authentication mechanisms, but must provide the capability for third-party products to be incorporated to provide additional authentication mechanisms. As such, FIA_UAU.5 is considered to be hierarchical to FIA_UAU.CCOPP. This means that a CCOPP-OS conformant TOE will satisfy the FIA_UAU.CCOPP requirement if it provides FIA_UAU.5 (and of course the operations are completed in a manner that is consistent with the CCOPP-OS requirement).

FIA_UAU.CCOPP.1: The TSF shall provide support for [assignment: *list of multiple authentication mechanisms*] to support user authentication.

FIA_UAU.CCOPP.2: The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

9.3 CLASS FPT – PROTECTION OF TOE SECURITY FUNCTIONS

9.3.1 Subset Inter-TSF Confidentiality During Transmission - FPT_ITC.CCOPP

This component is closely related to FPT_ITC.1, and hence is considered as part of an extended FPT_ITC family. It is identical in wording, except that it applies only to a defined subset of TSF data, and differs in the allocation of responsibility between TOE and remote trusted IT product. Note that FPT_ITC.1 is considered to be hierarchical to this extended component.

FPT_ITC.CCOPP.1: The TSF shall support the protection of [assignment: *list of TSF data*] transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

9.3.2 Subset Inter-TSF Integrity During Transmission - FPT_ITI.CCOPP

This component is closely related to FPT_ITI.1, and hence is considered as part of an extended FPT_ITI family. FPT_ITI.1.1 is not included. It is identical in wording to FPT_ITI.1.2, except that it applies only to a defined subset of TSF data, and differs in the allocation of responsibility between TOE and remote trusted IT product. Note that FPT_ITI.1 is considered to be hierarchical to this extended component.

FPT_ITI.CCOPP.1: The TSF shall support the capability to verify the integrity of [assignment: *list of TSF data*] transmitted between the TSF and another trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

APPENDIX A - ACRONYMS

CC	Common Criteria [for IT Security Evaluation]
CCOPP-OS	COTS Compartmentalized Operation PP
COTS	Commercial Off The Shelf
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
IT	Information Technology
MAC	Mandatory Access Control
NIST	National Institute of Standards and Technology
PP	Protection Profile
RBAC	Role Based Access Control
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

APPENDIX B – REFERENCES

[CAPP]   *Controlled Access Protection Profile,* version 1.d, 8 October 1999

[CC-V3.1]   *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 2, September 2007.

[CSPP]   *Guidance for COTS Security Protection Profiles*, version 0.4, February 2001

[CSPP-OS]   *COTS Security Protection Profile - Operating Systems*, version 1.0, January 2003

[LSPP]   *Labeled Security Protection Profile,* version 1.b, 8 October 1999

[RBAC]   *Role Based Access Control Protection Profile,* Version 1.0, July 30, 1998