

Solaris 10 11/06 Trusted Extensions **Security Target**

Version: 1.21 Public Release

Document Number: T10_101
Date: 4 June, 2008
Version: 1.21 Public Release

Abstract

This document is the Security Target for the EAL4+ Common Criteria v2.3 evaluation of Solaris10 Trusted Extensions developed by Sun Microsystems, Inc.



4150 Network Circle, Santa Clara, California, 94054

© 2008 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 U.S.A.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Solaris Management Console, Sun Ray, StarOffice, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. PostScript is a trademark or registered trademark of Adobe Systems, Incorporated, which may be registered in certain jurisdictions.

The OPEN LOOK and SunTM Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED 'AS IS' AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certaines composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Solaris Management Console, Sun Ray, StarOffice, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. PostScript est une marque de fabrique d'Adobe Systems, Incorporated, laquelle pourrait être déposée dans certaines juridictions. in the United States and other countries.



Please
Recycle

SUN MICROSYSTEMS, INC.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des États-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

References

Standards & Criteria

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, CCIMB-2005-08-002, August 2005

[CCP2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.3, CCIMB-2005-08-002, January 2005

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

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

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

[ALC_FLR] Part 2: Evaluation Methodology Supplement: Flaw Remediation, Version 1.1, February 2002

[NIST1] Letter from R. Chandramouli, re: FIA_UAU.2 in RBAC PP, Computer Security Division, NIST, dated 16 July 2001

[NIST2] Letter from R. Chandramouli, re: FPT_TST.1 in RBAC PP, Computer Security Division, NIST, dated 16 July 2001

Public Revision History

Version	Date	Author	Comments
1.21	June 2008	Jane Medefesser	Public Release

Contents

1	Introduction	1
1.1	ST Identification	1
1.2	ST Overview	1
1.3	CC Conformance	2
1.4	Structure	2
1.5	Terminology	2
1.6	Document Layout	5
2	TOE Description	7
2.1	Introduction	7
2.2	Intended Use	7
2.3	Evaluated Configurations	8
2.3.1	Target of Evaluation	8
2.3.2	File systems	9
2.3.3	Configurations	10
2.4	Summary of Security Features	12
2.4.1	DAC	13
2.4.2	MAC	13
2.4.3	Object Reuse	14
2.4.4	Identification and Authentication	14
2.4.5	Roles and Profiles	15
2.4.6	Security Management	15
2.4.7	Auditing	17
2.4.8	Enforcement	17
2.4.9	Secure Communication	17
2.4.10	TSF Protection	17
2.4.11	Privileges and Authorizations	18

2.4.12	Trusted Path	18
3	TOE Security Environment	19
3.1	Introduction	19
3.2	Threats	19
3.2.1	Threats countered by the TOE	20
3.2.2	Threats to be countered by measures within the TOE environment	20
3.3	Organizational Security Policies	21
3.4	Assumptions	22
3.4.1	Physical Aspects	22
3.4.2	Personnel Aspects	22
3.4.3	Procedural Aspects	23
3.4.4	Connectivity Aspects	23
4	Security Objectives	25
4.1	Security Objectives for the TOE	25
4.2	Security Objectives for the TOE Environment	26
5	Security Requirements	29
5.1	TOE Security Functional Requirements	29
5.1.1	Protection Profile SFRs Tailored for This ST	32
5.1.2	Security Audit (FAU)	33
5.1.3	User Data Protection (FDP)	33
5.1.4	Identification and Authentication (FIA)	35
5.1.5	Security Management (FMT)	37
5.1.6	Security Management Roles	38
5.1.7	Protection of the TSF (FPT)	38
5.1.8	Trusted Recovery	39
5.1.9	Specification of Management Functions	39
5.1.10	TOE Access	39
5.2	Additional SFRs for This ST	40
5.2.1	Security Management (FMT)	40
5.2.2	User Data Protection (FDP)	41



5.2.3	Trusted Path/Channels (FTP)	41
5.3	Strength of Function	42
5.4	TOE Security Assurance Requirements	42
5.5	Security Requirements for the IT Environment	42
5.5.1	OpenBoot PROM	42
5.5.2	System Controller (SC)	42
5.5.3	x86/x64 Workstations and Servers.	42
6	TOE Summary Specification	43
6.1	IT Security Functions	43
6.1.1	Discretionary Access Control (DAC)	43
6.1.2	Mandatory Access Control (MAC)	45
6.1.3	Object Reuse	48
6.1.4	Identification and Authentication	49
6.1.5	Session Locking	50
6.1.6	Secure Communication	50
6.1.7	Trusted Path.	50
6.1.8	Administration.	51
6.1.9	Audit	52
6.1.10	Enforcement Functions	55
6.1.11	Failure	55
6.2	Required Security Mechanisms	55
6.2.1	Identification and Authentication	55
6.3	Assurance Measures	56
7	Rationale	59
7.1	Correlation of Threats, Policies, Assumptions and Objectives.	59
7.2	Security Objectives Rationale	62
7.2.1	Complete Coverage - Threats	62
7.2.2	Complete Coverage - Policy	68
7.2.3	Complete Coverage - Environmental Assumptions	70
7.2.4	Complete Coverage - Personnel Assumptions	70
7.2.5	Complete Coverage - Procedural Assumptions	71

7.3	Security Requirements Rationale	73
7.3.1	Complete Coverage - Objectives	73
7.3.2	Requirements are Mutually Supportive and Internally Consistent	82
7.3.3	Justification for Choice of Assurance Requirements	83
7.3.4	Strength of Function Claim is Consistent with Security Objectives	83
7.4	TOE Summary Specification Rationale	83
7.4.1	IT Security Functions Satisfy Functional Requirements	84
7.4.2	Justification for Compliance of Assurance Measures	90
7.5	PP Claims and Rationale	91
7.5.1	PP Reference	91
7.5.2	PP Tailoring	91
7.5.3	PP Additions	91
7.5.4	PP Rationale	91
8	Appendix A	93
A 1.1	Platform 1 Configurations	93
A 1.2	Platform 2 Configurations	96
A 1.3	Platform 3 Configurations	97

1.1 ST Identification

Title: Solaris 10 11/06 Trusted Extensions Security Target version 1.21 Public Release

Keywords: Solaris 10 11/06, Trusted Extensions, general-purpose operating system, POSIX, UNIX.

This document is the Security Target (ST) for the CC evaluation of the Solaris 10 11/06 Trusted Extensions operating system product, and is conformant to the Common Criteria for Information Technology Security Evaluation [CC].

1.2 ST Overview

This Security Target documents the security characteristics of the Solaris 10 11/06 Trusted Extensions operating system. Solaris 10 11/06 Trusted Extensions is an optionally enabled layer of the Solaris 10 11/06 Operating System that provides security labeling technology allowing data security policies to be separated from data ownership.

The Solaris Operating Environment is a computer operating system, based on the open-source UNIX SunOS developed by Sun Microsystems, Inc.

Solaris is a highly-configurable UNIX-based operating system. Originally developed to meet the requirements of the C2 class of the U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria (TCSEC), it now meets specific equivalent Protection Profiles developed within the Common Criteria Project. These broad requirements are described for the Common Criteria scheme in the Controlled Access Protection Profile [CAPP] and the Role Based Access Control Protection Profile [RBAC]. Similarly, Solaris 10 11/06 Trusted Extensions has been developed to meet the requirements of the B1 class of the TCSEC, and now meets the equivalent Labeled Security Protection Profile [LSPP] in addition to the [CAPP] and [RBAC] by virtue of the underlying Solaris 10 11/06 operating system.

A Solaris 10 11/06 Trusted Extensions system consists of a number of workstations and/or servers linked together to form a single distributed system. Users share the resources of multiple workstations and/or servers connected together in a single, distributed Trusted Computing Base (TCB).

This Solaris 10 11/06 Trusted Extensions ST version 1.21 Public Release is based on the Solaris 10 11/06 ST 3.0 FINAL with the appropriate changes and addition of new material.

1.3 CC Conformance

This ST is conformant with the following:

- Controlled Access Protection Profile version 1.d [CAPP].
- Role Based Access Control Protection Profile version 1 [RBAC]
- Labeled Security Protection Profile version 1.b [LSPP]

This ST is Common Criteria for Information Technology Security Evaluation, version 2.3. Part 2 conformant and Part 3 conformant, augmented by ALC_FLR.3, with a claimed Evaluation Assurance Level of EAL4+.

1.4 Structure

The structure of this document is as defined by [CC] Part 1 Annex C.

- Section 2 is the TOE Description.
- Section 3 provides the statement of TOE security environment.
- Section 4 provides the statement of security objectives.
- Section 5 provides the statement of IT security requirements.
- Section 6 provides the TOE summary specification, which includes the detailed specification of the IT Security Functions.
- Section 7 provides the rationale for the security objectives, security requirements, TOE summary specification and PP claims against [CAPP], [RBAC] and [LSPP].
- Appendix A contains information about TOE supported hardware platforms

1.5 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Action: An action is an execution of a command or system call.

Administrative User: This term refers to an administrator of a Solaris 10 11/06 Trusted Extensions system. Administrators are granted a rights profile and may also be granted roles.

Audit Class: This is the name given to the definition of a collective grouping of events representing particular types of activity to be monitored; e.g. file read, network, administrative, application, process, file attribute modify, etc.

Authentication data: This includes a user identifier, password and authorizations for each user of the product.

BART: Basic Auditing and Reporting Tool: Used by system administrators to validate the integrity of data files and meta information (file ownership, size, and so on). Provides tools to monitor the integrity of all files on the system at any point in time.

CCATS: Commodity Classification Automated Tracking System. U.S. Bureau of Industry and Security code number for products classified against the Commerce Control List.

CB: Certification Body, a part of CSE (Communications Security Establishment) overseeing and monitoring evaluations in Canada.

CCS: Canadian Common Criteria Evaluation and Certification Scheme. The CC program run by the Government of Canada.

CDE: Common Desktop Environment. The legacy user desktop provided with the Solaris Operating System. It is an integrated graphical user interface built on top of the Motif toolkit (a graphical widget toolkit for building graphical user interfaces under the X Window System on UNIX and other POSIX-compliant systems).

Common Components: These relate to components of the mid-frame family that share the same or functionally similar hardware such as CPU, memory, Compact PCI Card, SC, I/O assemblies, etc.

Dynamic Reconfiguration (DR): This is the process of dynamically reconfiguring system boards, removing them or installing them onto a system while the Solaris operating environment is running. DR software is part of the Solaris Operating Environment and supports Multiple Domaining or Dynamic System Domains feature.

Dynamic System Domains: see Multiple Domain

FCS: First Customer Shipment.

JDS: Sun Java Desktop System. Sun's version of the opensource GNOME 2.0 Desktop Operating Environment. GNOME is a Unix and Linux desktop suite and development platform that provides a desktop for end-users, users. JDS is provided with Solaris 10 11/06 Trusted Extensions as a selectable option (an alternative to the Solaris CDE – Common Desktop Environment).

High End Server platforms: For the purposes of this ST this means the Sunfire 12K, 15K, 20K and 25K servers.

IARR: Impact Analysis and Rationale Report, the document which shows platform equivalency across the SunFire mid-frame range of servers.

Low-end/Entry-Level platforms: For the purposes of this ST this means the following product models: Servers E3500, E4500, E420R, E450, E250 and E220R; Workstation; Ultrasparcs 25, 30, 45, 60, 80 and 450; SunBlades 100, 150, 1000, 1500, 2000 and 2500; Netra X1, 20, 120, 240, CT410, CT810 and CT820; SunFire B100s, V100, V120, V125, V215, V245, V280R, V445, V480, V880, V880z, V210, V240, V250, V440; Netra 440 Server; UltraSparc 5 & 10; and the Ultra 3 Mobile. Entry level platforms also include all of Sun's Opteron- and Intel-based machines: the Sunfire v20z, v40z, x2100, x2100 M2, x2200 M2, x4100, x4100 M2, x4200, x4200 M2, x4500, x4600, x4600 M2 and servers; the Dell Poweredge 6000 workstation; the Ultra 20 and Ultra 20 M2 workstations; and the Javastations W1100 and W2100.

Mid-frame/Mid-range platforms: For the purposes of this ST this means the E10K Server; the Netra 1280; the Sunfire 1280, 3800, 4800, 4810, E5500, E6500, and 6800 servers; the SunFire V490, V890, 2900, 4900, 6900, T1000, T2000 Servers; and the Netra T2000 Server and CP3060 Blade.

Multiple Domain (MD): This is a hardware configuration feature whereby a system may be logically partitioned into one or more domains. Each domain is a self-contained server of one or multiple system boards, contains CPU, memory, I/O, boot-disk, network resources and runs a single instance of the Solaris Operating Environment.

Object: In Solaris 10 11/06 Trusted Extensions, objects belong to one of four categories: file system objects, other kernel objects (such as processes, programs and interprocess communication), window system objects and miscellaneous objects.

Peripherals: This term should be taken to mean (optional) storage, communications or printing devices that can be used with the TOE platforms.

Platform: Refers to servers, workstations or both when contextually appropriate.

PP: Protection Profile.

Product: The term product is used to define all hardware and software components that comprise the distributed Solaris 10 11/06 Trusted Extensions system.

Public object: A type of object for which all subjects have read access, but only the TCB has write access.

SB: Sun Blade, a name given to a family of workstation products.

SC: System Controller, the component in the mid-frame platforms that boots up the ToE, and performs similar functions to that of an Open BootPROM

Security Attributes: As defined by functional requirement FIA_ATD.1, the term 'security attributes' includes the following as a minimum: user identifier; group memberships; user authentication data.

Server: A computer/device which provides/manages information or services to computers on a network.

SF: Security Function OR (alternatively) SunFire, a name given to a family of servers, dependent upon context.

SFR: Security Functional Requirement

SMC: Sun Management Console, a secure system management GUI for administration

SoF: Strength of Function

SPARC: The name given to the processor family that is incorporated into the platforms identified in this ST.

SRN: Security Release Notes, see references.

Subject: There are two classes of subjects in Solaris 10 11/06 Trusted Extensions:

- *untrusted subject* - this is a Solaris 10 11/06 Trusted Extensions process running on behalf of some user, running outside of the TCB (for example, with only basic privileges).
- *trusted subject* - this is a Solaris 10 11/06 Trusted Extensions process running as part of the TCB (for example, with more than just basic privileges). Examples are service daemons and the processes implementing the windowing system.

System: Includes the hardware, software and firmware components of the Solaris 10 11/06 Trusted Extensions product which are connected/networked together and configured to form a usable system.

System Controller: This is an embedded system consisting of the system controller board and the system controller software (own processor, memory, etc.) which provides communication pathways between the platform system components and additionally performs functions replicating those of an ‘Open Boot PROM’.

Target of Evaluation (TOE): The TOE is defined as the Solaris 10 11/06 Operating System with Trusted Extensions, running and tested on the hardware and firmware specified in this ST. The BootPROM firmware forms part of the TOE Environment (see section 5.4).

Trusted Computing Base (TCB): A TCB is the totality of protection mechanisms within a computer system (which may include a combination of hardware, firmware, and software) that is responsible for enforcing a security policy

TSF: TOE Security Function.

TSP: TOE Security Policy.

User: Any individual/person who has a unique user identifier and who interacts with the Solaris 10 11/06 Trusted Extensions product.

Workstation: A workstation is a computer intended for individual use that is more capable, powerful and faster than a personal computer.

1.6 Document Layout

IT security functions are assigned a unique reference identifier of the form Name.1 to enable ease of reference. For example, DAC.1, Audit.1.

This Page Intentionally Left Blank

2.1 Introduction

The TOE description aims to aid the understanding of the TOE's security requirements and provides a context for the evaluation. It defines the scope and boundaries of the TOE, both physically and logically, and describes the environment into which the TOE will fit.

For the purposes of this ST, the TOE is the Sun Microsystems Solaris 10 11/06 Operating System with Trusted Extensions, referred to throughout this document as "Solaris 10 11/06 Trusted Extensions", "Trusted Extensions" or "the TOE".

2.2 Intended Use

Solaris 10 11/06 is a highly-configurable UNIX-based operating system which has been developed to be compliant with the Controlled Access and Role Based Protection Profiles. Originally developed to meet the requirements of the C2 class of the U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria (TCSEC), it now meets specific equivalent Protection Profiles developed within the Common Criteria Project. Solaris 10 11/06 Trusted Extensions builds on Solaris 10 11/06 and was originally developed to meet the requirements of the B1 class of the TCSEC and is now compliant with the specific equivalent Common Criteria Protection Profiles.

The TOE consists of a number of workstations and/or servers linked together to form a single distributed system. Users share the resources of multiple workstations and/or servers connected together in a single, distributed Trusted Computing Base (TCB). After successful login, the users have access to a general computing environment, allowing the start-up of user applications, issuing user commands at shell level, creating and accessing files. The TOE provides adequate mechanisms to separate the users and protect their data. Privileged commands are restricted to the system administrator role.

The TOE permits one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled shared access to the data stored on the system. Such installations are typical of personal, workgroup, or enterprise computing systems accessed by users local to, or with otherwise protected access to, the computer systems.

The TOE provides facilities for on-line interaction with users. Networking is covered only to the extent to which the TOE can be considered to be part of a centrally-managed system that meets a common set of security requirements. It is assumed that responsibility for the safeguarding of the data protected by the TOE can be delegated to the TOE users (other than the management of TOE security critical parameters, which is performed by administrative users). All data is under the control of the TOE. The data is stored in named objects, and the TOE can associate with each controlled object a description of the access rights to that object.

All individual users of the TOE are assigned a unique user identifier; this unique identifier type supports individual accountability. The TOE authenticates the claimed identity of each user before allowing a user to perform any further actions. The TOE enforces controls such that access to data objects can only take place in accordance with the access restrictions.

2.3 Evaluated Configurations

2.3.1 Target of Evaluation

This section defines the software that comprises the TOE and the Servers/Workstations that the software runs on.

2.3.1.1 TOE Certification Platforms:

Note that the UltraSPARC II, Iii, Iie, III, and IIIi Low-End platforms use an OpenBoot PROM. SunFire MidFrame and High-End platforms make use of the System Controller component to perform similar tasks to the OpenBOOT PROM. Both the OpenBoot PROM and System Controller are outside of the scope of this evaluation. The OpenBootPROM and System Controller are protected by a password commensurate with the appropriate SoF requirement for the environment. The Administrator is responsible for selecting passwords of appropriate strength to meet the ST requirements.

Workstations and Servers:

The target of evaluation is a (distributed) operating system product running on:

- Platform 1: Entry Level workstations and servers utilizing an UltraSPARC II, UltraSPARC Iie, UltraSPARC Iii, UltraSPARCIII, UltraSPARCIIIi, or UltraSPARC T1 processor in a single or multiple configuration. Various configurations of these platforms are possible and the evaluation scope includes all possible combinations/permutations through the testing of CB appropriate configurations. An [IARR], Impact Analysis and Rationale Report, will show platform equivalency across the SunFire midframe family.
- Platform 2: The Netra 1280 and SunFire mid-frame and high-end family offering Dynamic Reconfiguration and Multiple Domaining as defined in Section 1.5 and utilizing an UltraSPARC III Cu (copper based) or UltraSPARC IV processor. Various configurations of these platforms are possible and the evaluation scope includes all

possible combinations/permutations through the testing of CB appropriate configurations. An [IARR], Impact Analysis and Rationale Report, will show platform equivalency across the SunFire midframe family.

- Platform 3: AMD based processor systems: AMD Opteron 800, 1200, and 8000 series; AMD-64 100, 200, and 2000 series; AMD dual-core 1200 and 2000 series; AMD Opteron 285; and, Intel Xeon.

Please refer to Appendix A for tables illustrating the hardware configurations available for use. Note that within each platform group, the processor speed associated with each model is dependant upon what was or is offered by the vendor.

2.3.1.2 Software

The Target of Evaluation is based on the following system software:

- Solaris 10 11/06
- Solaris Management Console 2.1 (SMC)
- Trusted Extensions add-on software available in the extra-value directory of the Solaris 10 11/06 DVD
- Sun Java System Directory Server 6.2 version LDAP naming server

The TOE documentation is available on SUN's website:

<http://www.sun.com/software/security/securitycert>.

2.3.2 File systems

The following filesystem types are supported:

- the standard Solaris UNIX filesystem, ufs;
- the standard Network File System access protocol, nfs (V2, V3, and V4);
- the MS-DOS formatted filesystem pcfs;
- the High Sierra filesystem for CD-ROM drives, hfsf;
- the Loopback File System, lofs. This feature allows directories to be mounted multiple times in different ways (e.g., read-only or read-write);
- the Solaris Zettabyte File System (Solaris ZFS). This feature provides enhanced file system capabilities by automating common administrative tasks, protecting data from corruption and providing an extremely high degree of scalability. Solaris ZFS utilizes virtual storage pools to simplify expanding or contracting of file systems via additional drives.

In addition to the above file systems a number of "internal" filesystems are supported: The file descriptor file system, fd, allows programs to access their own file descriptors through the file name space, such as /dev/stdin corresponding to /dev/fd0.

- The names file system, namefs (or namfs) allows the arbitrary mounting of any file descriptor on top of another file name.
- The doors file system, doorfs allows fast control transfer between processes on the same machine.
- The process file system, procs (/proc), provides access to the process image of each process on the machine as if the process were a “file”. Process access decisions are enforced by DAC attributes inferred from the underlying process' DAC attributes.

2.3.3 Configurations

The evaluated configurations are defined as follows.

- When installing the product, the entire distribution should be selected.
- The evaluated version (or “package set”) must be selected at time of installation in accordance with the description provided in the documentation and installed accordingly.
- No additional SMC add-ons should be installed.
- Minimum physical memory and disk configurations provided for the hardware in the tables in Appendix A are provided with the Solaris 10 11/06 documentation and may not be sufficient for all applications. For components which must be installed separately from the Solaris Installation, please consult that component's installation guide to determine requirements.
- The default setting for the Global Zone (Solaris Container) should be used. In addition, when configuring non-global Zones, the non-global Zone root file system models should be followed (sparse root Zone model and the whole root Zone model).
- The evaluated configuration includes both the Common Desktop Environment (CDE) windowing environment and Sun Trusted Java Desktop System (TJDS) Operating Environment. Users may select either of these during login via the “User Preference” screen.

Application note: for the CC evaluated version of Trusted Extensions, the JDS/GNOME accessibility features are not available.

- Trusted Extensions supports the use of IPv4 and IPv6.
- Trusted Extensions supports the use of DHCP, (no additional security claims are made for DHCP).
- 64 bit architectures are included.
- Web Based Enterprise Management Services (WBEM) are included (no additional security claims are made for WBEM).
- Web Start, Jumpstart, DVD and CD installations are all supported.
- The standard Service Management Framework (SMF) profiles, generic.xml and generic_limited_net.xml, must be used.
- BART (Basic Auditing and Reporting Tool) must be correctly configured to collect and compare attributes of filesystem objects installed on the system.
- Trusted Extensions supports the use of the Solaris Pluggable Authentication Module (PAM) using the default configuration for identification and authentication.
- If the system console is used, it must be connected directly to the server/workstation and afforded the same physical protection as the server/workstation.

The product comprises one or more of the listed servers and/or workstations (and optional peripherals) running the above listed system software (a platform running the above listed software is referred to as a “TOE platform” below).

If the product is configured with more than one TOE platform, they are linked by Ethernet LANs, which may be joined by bridges/routers or by TOE platforms which act as routers/gateways.

If other systems are connected to the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE. All links from this network to untrusted networks (e.g., the Internet) need to be protected by appropriate measures like carefully configured firewall systems that prohibit attacks from the untrusted networks. Those protections are not part of the TOE environment.

No other processors may be connected to the Ethernet network, except as noted below.

If the product is configured with more than one TOE platform, then the Sun Java System Directory Server 6.2 version of the LDAP naming service must be used and the Sun Java System Directory Server 6.2 version LDAP naming server(s) must be TOE platforms.

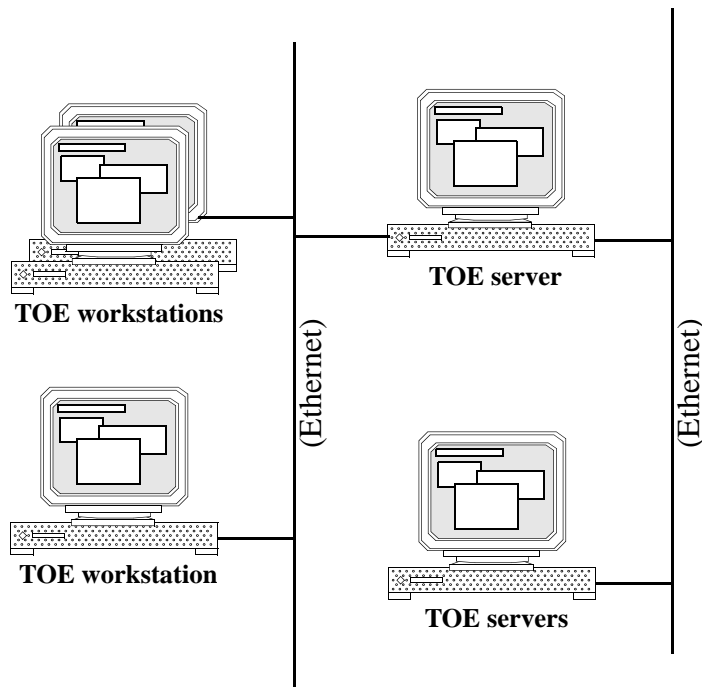


Figure 2-1 Typical Evaluation Configuration

2.4 Summary of Security Features

The primary security features of the product are:

- Discretionary Access Control;
- Mandatory Access Control;
- Object Reuse;
- Identification and Authentication (Including PAM);
- Roles and Profiles (Including Service Management Framework);
- Security Management;
- Auditing;
- Enforcement;
- Secure Communication;
- TSF Protection;
- Privileges and Authorizations; and,
- Trusted Path.

These primary security features are supported by kernel and process domain separation and reference mediation, which ensure that the features are always invoked and cannot be bypassed.

2.4.1 DAC

Discretionary Access Control (DAC) restricts access to objects, such as files, based on Access Control Lists (ACLs) that include the standard UNIX permissions for user, group and other users. Access control mechanisms also protect System V IPC (interprocess communication) objects from unauthorized access.

The Trusted Extensions ACL model allows authorized users to grant access rights, to a user or group, that govern who can access a specific object, a group of properties, or an individual property of an object.

2.4.2 MAC

Trusted Extensions extends the underlying Solaris 10 11/06 security model with a Mandatory Access Control (MAC) policy. The MAC policy applies to all aspects of the operating system, including:

- **Mandatory File and Device Access Controls,**
- **Trusted Networking,**
- **Trusted Printing, and**
- **Trusted Windows.**

Each device (file system, terminal, disk drive, printer, network, etc.) and user is assigned sensitivity labels. These sensitivity labels are used for making MAC policy decisions.

Trusted Extensions uses Zones (see Section 2.4.6) to virtualize application environments for each sensitivity label. With the exception of the Global Zone which is restricted to users with an administrative role, each zone is associated with a single sensitivity label. When users log in, they are associated with the zones that corresponded with their selected sensitivity labels. Each process that runs within a zone is implicitly labeled with the sensitivity label of the zone and has access only to resources (objects) that are also associated with the zone.

Files are not individually labeled, but rather are labeled at the granularity of their hosting filesystem. Each filesystems, in turn, is labeled on the basis of the zone associated with that file system. A zone can mount its own filesystems read-write, but can mount filesystems with other sensitivity labels (from other zones) read-only and only when allowed by the MAC policy rules.

Similarly, a given zone can only connect to networks, printers, or other devices that are allowed based on the MAC policy rules. Once connected, processes executing in a given zone can access only those connected devices. As such, MAC policy conformance is ensured when devices are connected rather than when they are used.

There are some privileges that can be granted that allow exceptions to be made relative to the MAC policy. Those privileges can be granted to users so they will be available to processes executing on behalf of those users, but privileges are further limited by zone definitions. Each zone can be assigned privileges which serve as a mask to limit privileges available to processes executing in that zone. No process, even root, executing in a zone can utilize privileges that are not assigned to both the process and the zone. In a typical application, only the Global Zone would be assigned the full

range of privileges so the individually labeled zones can be more effectively controlled. In addition, privileges would typically be assigned to users via roles (see Section 2.4.5).

In addition to the MAC policy controls, networks and printers have additional MAC-related features.

Trusted Extensions provides labeling of network traffic using CIPSO labels. Network connections are either single level or multi-level. Trusted Extension automatically labels single-level network traffic with the sensitivity label of the corresponding zone. In the case of multi-level network ports, network traffic must be explicitly labeled by the corresponding multi-level application. When network traffic is received it is directed to the zone or multi-level application based on its sensitivity label and network address.

Trusted Extensions also provides labeling of printed output based on the sensitivity label of the data being printed.

Trusted Extensions includes trusted windows features where individual windows are labeled and must be within the range of sensitivity labels allowed to the corresponding user. Data transfer operations among windows is controlled in accordance with the MAC policy rules.

2.4.3 Object Reuse

Object Reuse functionality ensures that memory and other storage and file system objects are cleared of data (i.e. Contain no data) when they are re-allocated or re-used.

2.4.4 Identification and Authentication

Trusted Extensions provides identification and authentication as a built-in feature using the Pluggable Authentication Module (PAM) based on usernames and passwords.

The PAM modules that are included in the default installation are included in the evaluated configuration. The list of PAM modules includes:

```
pam_authtok_check.so.1
pam_authtok_get.so.1
pam_authtok_store.so.1
pam_dhkeys.so.1
pam_dial_auth.so.1
pam_passwd_auth.so.1
pam_rhosts_auth.so.1
pam_roles.so.1
pam_tsol_account.so.1
pam_unix_account.so.1
pam_unix_auth.so.1
pam_unix_cred.so.1
pam_unix_session.so.1
```

In cooperation with the Simple Authentication and Security Layer (SASL) and the Generic Security Service (GSS); PAM is the mechanism available for both distributed and non-distributed authentication. Note: LDAP is used with SASL.

Trusted Extensions provides the mechanisms for password policy, as defined by an administrator (e.g., minimum length), enforcement.

2.4.5 Roles and Profiles

Trusted Extensions supports the concept of Roles, allowing administrative powers to be broken into many discrete Roles. This removes the requirement of one superuser (root or only one system-administrator) to administer the TOE. A Role consists of a set of Rights profiles. Rights Profiles can be populated with the required authorizations appropriate to the defined role, thus allowing the administrative functionality to be distributed and hence diluted amongst the Roles, to reduce the impact of any misuse of a Role.

Trusted Extensions includes the Service Management Framework (SMF) which provides RBAC authorization that is required to administer services. SMF allows administrators to install, configure and enable system applications and provides dependency based service startup/recovery. SMF can be used to assign uid/gid/default and limit privileges for services.

SMF also provides for distinction between services and applications that are configured/enabled (e.g., services can be fully configured but disabled or enabled/disabled temporarily or permanently).

There are 2 types of SMF profiles:

- **generic_open.xml:** most services enabled (similar to Solaris 9); and
- **generic_limited_net.xml:** fewer remotely available network services enabled, only ssh available for remote login, most other services off

2.4.6 Security Management

The management of the security critical parameters of the TOE is performed by administrative users. A set of commands that require privileges are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by non-administrative users.

Trusted Extensions includes Solaris Zones (formerly N1 grid containers). Solaris Zones provide an advanced resource management feature which ensures that applications can be run in separate Zones, with logical isolation ensuring true encapsulation. Zones provide multiple virtualized application environments from a single Solaris kernel to provide (in addition to process containment) resource usage & security isolation but blocks direct access to hardware (each zone appears as a separate hosts from “outside”).

The virtual server in the zone hides the system details. The hardware on which the zone is running is not exposed to the applications or users. Solaris Zones allows for a separate uid /gid namespace per zone, and each zone has its own separate file system space and processes executing in that zone are limited by privileges configured for that zone.

The upper limit for the number of zones on a system is 8192. The number of zones that can be effectively hosted on a single system is determined by the total resource requirements of the application software running in all of the zones.

There are 2 standard types of Solaris Zones, global and non-global. A global zone has a dual function as it is both the default zone for the system and the zone used for system-wide administrative control. All processes run in the global zone if no non-global zones (referred to simply as “zones”) are created by the global administrator.

The global zone is the only zone from which a non-global zone can be configured, installed, managed, or uninstalled. Only the global zone is bootable from the system hardware. Administration of the system infrastructure, such as physical devices, routing tables, or dynamic reconfiguration (DR), is only possible in the global zone. Appropriately privileged processes running in the global zone can access objects associated with other zones.

A non-global zone provides isolation at almost any level of granularity required. A zone does not need a dedicated CPU, a physical device, or a portion of physical memory. These resources can either be multiplexed across a number of zones running within a single domain or system, or allocated on a per-zone basis using the resource management features available in the operating system.

Each zone can provide a customized set of services. To enforce basic process isolation, a process, without special privileges, can see or signal only those processes that exist in the same zone. Basic communication between zones is accomplished by giving each zone at least one logical network interface. An application running in one zone cannot observe the network traffic of another zone. This isolation is maintained even though the respective streams of packets travel through the same physical interface.

Each zone is given a portion of the file system hierarchy. Because each zone is confined to its subtree of the file system hierarchy, a workload running in a particular zone cannot access the on-disk data of another workload running in a different zone.

Files used by naming services reside within a zone's own root file system view. Thus, naming services in different zones are isolated from one other and the services can be configured differently.

There are two types of non-global zone root file system models: sparse and whole root. The sparse root zone model optimizes the sharing of objects. The whole root Zone model provides the maximum configurability. Note that whole root zones are not recommended and the sparse model (SUNWtsoldef) should be used.

Zone Security Properties:

- Services can be isolated from each other;
- Potentially risky software can be quarantine;
- Processes in Zones can't send signals to other Zones (even if they have `proc_session` or `proc_owner`);
- System memory cannot be shared between Zones;
- Untrusted parties can be isolated to contain potential damage by a breach; and
- Each Zone can only see those processes running within it (except Global Zone)

In addition, each "Global Zone" can:

- Observe all activities inside each Zone (but only if the process has sufficient privileges to do so);
- Not be seen by software in a non global zone (note: non-global zones run with less privileges, which will be a subset of the available privileges); and
- Change the contents or processes in each zone (but only if the process has sufficient privileges to do so).

2.4.7 Auditing

Trusted Extensions can collect extensive auditing information about security related actions taken or attempted by users, ensuring that users are accountable for their actions. For each such action or event an audit record is generated containing: date and time of the event, user, security attributes and success or failure. This audit trail can be analyzed to identify attempts to compromise security and determine the extent of the compromise.

2.4.8 Enforcement

The Trusted Extensions security policy is enforced in a manner which ensures that the organizational policies are upheld in the target environment i.e. the integrity of the TSF is protected, kernel and process domain separation is enforced and bypass of the security functions is prevented.

2.4.9 Secure Communication

In its evaluated configuration, Trusted Extensions supports trusted communication channels for TCP and IP layer connections between different physical TOEs through different protocols/services.

2.4.10 TSF Protection

While in operation, the kernel software and data are protected by the hardware memory protection mechanisms. The memory and process management components of the kernel ensure a user process cannot access kernel storage or storage belonging to other processes.

Access to system services is controlled by the system, which requires that subjects wanting to perform security-relevant tasks be authorized appropriately.

Non-kernel TSF software and data are protected by DAC and process isolation mechanisms. In the evaluated configuration, the reserved user ID root owns the directories and files that define the TSF configuration. In general, files and directories containing internal TSF data (e.g., configuration files, batch job queues) are also protected from reading by DAC permissions.

The TOE and the hardware and firmware components are required to be physically protected from unauthorized access. The system kernel mediates all access to the hardware mechanisms themselves, other than program visible CPU instruction functions.

The TOE provides a tool that allows an administrative user to check the correct operation of the underlying hardware. This tool performs tests to check the system memory, the memory protection features of the underlying processor and the correct separation between user and supervisor state.

2.4.11 Privileges and Authorizations

Privileges and Authorizations are two separate mechanisms that confer security rights to processes and users respectively. Authorizations apply to users. In order for a user to perform an action that would otherwise be prohibited by the Trusted Extensions security policy, the user must have an authorization. Similarly, privileges, which apply to processes, are used to enable the process to perform an action that would otherwise be prohibited by the Trusted Extensions security policy.

2.4.12 Trusted Path

Trusted Extensions extends the underlying Solaris 10 11/06 security model with a Trusted Path mechanism. This mechanism, built into the trusted window capabilities of Trusted Extensions, provides a means to execute trusted applications in the context of the Global Zone and provide positive confirmation of that to the user so that they cannot be readily spoofed (e.g., by an untrusted or malicious program). Within the trusted window, visible to the user on their display, a trusted path indicator is protected so that it cannot be changed or overlaid by any user applications and the indicator indicates specifically when the user has currently selected, on the display, a running trusted application or not. Trusted applications accessible via the Trusted Path are provided for essentially all security management operations.

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

To this end, the statement of the TOE security environment identifies the lists and the assumptions made on the operational environment (including physical and procedural measures) and the intended method of use of the for the product, defines the threats that the product is designed to counter, and the organizational security policies with which the product is designed to comply.

Throughout this section, items that have been included which satisfy the specific requirements of the PPs are indicated with either [RBAC], [CAPP], or [LSPP] at the end of the item entry, where applicable.

3.2 Threats

The assumed security threats are listed below.

The **IT assets** to be protected comprise the information stored, processed or transmitted by the TOE. The term “information” is used here to refer to all data held within a workstation/server, including data in transit between workstations/servers.

The TOE counters the general threat of unauthorized access to information, where “access” includes disclosure, modification and destruction.

The **threat agents** can be categorized as either:

- unauthorized users of the TOE, i.e. individuals who have not been granted the right to access the system; or
- authorized users of the TOE, i.e. individuals who have been granted the right to access the system.

The threat agents are assumed to originate from a well managed user community in a non-hostile working environment, and hence the product protects against threats of inadvertent or casual attempts to breach the system security. The TOE is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security.

The threats listed below are grouped according to whether or not they are countered by the TOE. Those that are not countered by the TOE are countered by environmental or external mechanisms.

3.2.1 Threats countered by the TOE

[T.ACCESS_INFO] An authorized user of the TOE accesses information without having permission from the person who owns, or is responsible for, the information. In this context “access” is to be interpreted as observing information for which the user has no “need to know”, even though that user may have sufficient clearance to see the information. [RBAC]

[T.ACCESS_TOE] An unauthorized user of the TOE gains access to the system, thereby gaining unauthorized access to information. An unauthorized user of the TOE could gain access to the system by impersonating an authorized user, or by gaining access to an unattended platform at which an authorized user is logged on. Failure to detect the fact that an attack is taking place, or that many attempts have taken place over a period of time, may result in the attack eventually succeeding, resulting in the attacker gaining unauthorized access to information. [RBAC]

Note: T.ACCESS_TOE is meant to satisfy the T.ENTRY threat requirement from [RBAC].

[T.MODIFY] Unauthorized modification or destruction of information by an authorized user of the TOE. In this context “unauthorized” means not having the explicit or implicit permission of the designated owner of the information.

[T.ADMIN_RIGHTS] Unauthorized use of facilities which require administration rights by an authorized user of the TOE. Unauthorized use of such facilities by a user who cannot be trusted not to misuse them (whether intentionally or accidentally) could be exploited to gain unauthorized access to information.

[T.COMPROMISE] Data may be compromised in terms of confidentiality and integrity if an unauthorized User intercepts a communication link between the TOE and another trusted IT product (which may be another instantiation of the TOE) and attempts to modify information in a way that can not be detected by the TOE or the other trusted IT product.

3.2.2 Threats to be countered by measures within the TOE environment

The following threats apply in environments where specific threats to distributed systems need to be countered.

[T.TRANSIT] Data transferred between platforms is disclosed to or modified by unauthorized users or processes either directly or indirectly (e.g. through spoofing of workstation/server identity).

[T.OPERATE] Compromise of the IT assets may occur because of improper administration and operation of the TOE. Users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain logical access to and perform operations on its resources in breach of any permissions they may have. Potential attackers may seek to develop methods whereby the improperly administered security functions of the TOE may be circumvented during normal operation.[RBAC]

[**T.ROLEDEV**] The development and assignment of user roles may be done in a manner that undermines security. In general, roles could be developed which have an incorrect or improper combination of authorizations to perform operations on objects. In addition, users could be assigned to roles that are incommensurate with their duties, giving them either too much or too little scope of authorization. A particular concern arises in that users could be assigned conflicting roles with respect to ‘separation of duties’. An individual user could be authorized to perform multiple operations on data objects that represent the parts of a transaction that should be separated among different individuals. [RBAC]

3.3 Organizational Security Policies

The TOE complies with the following organizational security policies:

[**P.AUTH**] Only those users who have been authorized to access the information within the system may access the system.[CAPP][LSPP]

[**P.DAC**] The right to access specific data objects is determined on the basis of:

- a. the owner of the object; and
- b. the identity of the subject attempting the access; and
- c. the implicit and explicit access rights to the object granted to the subject by the object owner.[RBAC]

Note: P.DAC is meant to satisfy the P.ACCESS policy requirement from [RBAC].

[**P.ACCOUNTABLE**] The users of the system shall be held accountable for their actions within the system.[CAPP][LSPP]

[**P.NEED_TO_KNOW**] The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a “need to know” for that information. [CAPP][LSPP]

[**P.MAC**] The system must limit the access to information based on sensitivity, as represented by a label, of the information contained in objects, and the formal clearance of users, as represented by subjects, to access that information. The access rules enforced prevent a subject from accessing information which is of higher sensitivity than it is operating at and prevent a subject from causing information from being downgraded to a lower sensitivity.

The method for classification of information is made based on criteria set forth by the 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 classification of information is outside the scope of the IT system; the IT system is only expected to enforce the classification rules, not determine classification.

The method for determining clearances is also outside the scope of the IT system. It is essentially based on the trust placed in individual users by the organization.[LSPP]

3.4 Assumptions

This section indicates the minimum physical and procedural measures required to maintain security of the TOE.

3.4.1 Physical Aspects

[A.PROTECT] The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification by potentially hostile outsiders.

It is assumed that all software and hardware, including network and peripheral cabling is approved for the transmittal of the most sensitive data held by the system. Such items are assumed to be physically protected against threats to the confidentiality and integrity of the data transmitted. [RBAC][CAPP][LSPP]

[A.LOCATE] The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access. [RBAC][CAPP][LSPP]

[A.ASSET] It is also assumed that the value of the stored assets merits moderately intensive penetration or masquerading attacks. It is also assumed that physical controls in place would alert the system authorities to the physical presence of attackers within the controlled space. [RBAC]

3.4.2 Personnel Aspects

[A.ACCESS] Rights for users to gain access and perform operations on information are based on their membership in one or more roles (and the profiles that accompany these roles). These roles are granted to the users by the TOE Administrator. These roles accurately reflect the users job function, responsibilities, qualifications, and/or competencies within the enterprise. [RBAC]

[A.MANAGE] There will be one or more competent and trustworthy individuals assigned to manage TOE security. These individuals will have sole responsibility for the following functions:

- a. Create and maintain roles;
- b. Establish and maintain relationships among roles; and
- c. Assignment and Revocation of users to roles.

In addition these individuals (as ‘owners of the entire corporate data’), along with object owners will have the ability to assign and revoke object access rights to roles. [RBAC][CAPP][LSPP]

[A.OWNER] A limited set of users is given the rights to “create new data objects” and they become owners for those data objects. The organization is the owner of the rest of the information under the control of TOE. [RBAC]

[A.NO_EVIL_ADM] The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation. [CAPP][LSPP]

[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. [CAPP][LSPP]

3.4.3 Procedural Aspects

[A.USER] Each individual user is assumed to have a unique user ID.

[A.PASSWORD] Those responsible for the TOE must configure minimum password length for normal users to be at least 8 characters.

[A.CLEARANCE] Procedures exist for granting users authorization for access to specific security levels. [LSPP]

[A.SENSITIVITY] Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all output generated. [LSPP]

3.4.4 Connectivity Aspects

[A.LDAP_DOMAINS] It is assumed that, if the product comprises more than one platform, all platforms are administered from a central point within each LDAP directory domain.

LDAP allows the creation of multiple administrative domains, thus allowing administrators to control local resources and user accounts, yet making it possible for users and resources to operate seamlessly over the entire organization.

[A.BRIDGES&ROUTERS] All bridges and routers are assumed to correctly pass data without modification.

[A.CONNECT] All connections to peripheral devices reside within the controlled access facilities. CAPP/LSPP/RBAC-conformant TOEs address security concerns related to the manipulation of the TOE through its legitimate interfaces. Internal communication paths to interfaces points such as terminals are assumed to be adequately protected. [RBAC][CAPP][LSPP]

[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. CAPP and LSPP-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. [CAPP][LSPP]

This Page Intentionally Left Blank

4.1 Security Objectives for the TOE

Throughout this section, items that have been included which satisfy the specific requirements of the PPs are indicated with either [RBAC], [CAPP], or [LSPP] at the end of the item entry, where applicable.

[O.AUTHORIZATION] The TOE must ensure that only authorized users gain access to the TOE and its resources. [CAPP][LSPP]

[O.ENTRY] The TOE must prevent logical entry to it by persons or processes with no rights to access it.[RBAC]

[O.DISCRETIONARY_ACCESS] The TOE must control access to resources based on the identity of users. The TSF must allow authorized users to specify which resources may be accessed by which users.

The TOE must provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the P.DAC security policy. [CAPP][LSPP]

[O.MANDATORY_ACCESS] The TSF must control access to resources based upon the sensitivity and categories of the information being accessed and the clearance of the subject attempting to access that information. [LSPP]

[O.KNOWN] Legitimate users of the system must be identified before rights of access can be granted. RBAC assumes that there is a finite community of known users who will be granted rights of access and that system management has authority over that user community. [RBAC]

[O.AUDITING] The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators. The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise. [RBAC][CAPP][LSPP]

[O.ACCOUNT] The TOE must ensure that all users can be held accountable for their security relevant actions. [RBAC]

[O.TRUSTPATH] The TSF must be designed and implemented in a manner that allows for establishing a trusted channel or communication path between the TOE and another trusted IT product that protects the user data transferred over this channel from disclosure and undetected modification.

[O.RESIDUAL_INFO] The TOE must ensure that any information contained in a protected resource is not released when the resource is recycled. [CAPP][LSPP]

[O.MANAGE] The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality. [RBAC][CAPP][LSPP]

Note: O.MANAGE is meant to satisfy the O.ADMIN objective from [RBAC].

[O.ENFORCEMENT] The TOE security policy is enforced in a manner which ensures that the organizational policies are enforced in the target environment i.e. the integrity of the TSF is protected. [CAPP][LSPP]

[O.DUTY] The TOE must provide the capability of enforcing the separation of duties, so that no single user is required to perform all administrative functions. [RBAC].

[O.HIERARCHICAL] The TOE must allow hierarchical definitions of profile rights. The hierarchical definition of rights gives the ability to define profile rights in terms of other profile rights. [RBAC].

[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. [RBAC]

4.2 Security Objectives for the TOE Environment

[O.E_ADMIN] Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

[O.E_ACCOUNTABLE] Those responsible for the TOE must ensure that:

a.The product is configured such that only the approved group of users for which the system was accredited may access the system.

b.Each individual user is assigned a unique user ID.

[O.E_AUDITDATA] Those responsible for the TOE must ensure that the audit functionality is used and managed effectively. In particular:

a.Procedures must exist to ensure that the audit trail for the product (i.e., all networked components containing an audit trail) is regularly analyzed and archived, to allow retrospective inspection.

b.The auditing system must be configured such that the loss of audit data is minimized upon:

-planned or unplanned shutdown; or

-lack of available audit storage (in particular administrators should ensure that the AUDIT_CNT flag is correctly set as identified in the Administration documentation supplied with the TOE, and that remote partitions are mounted with the appropriate option [noac] so that audit information is not lost when the partition fills).

c. The auditing system is designed such that bad authentication data will not be stored in the audit trail.

d. The media on which audit data is stored must not be physically removable from the platform by unauthorized users.

[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 IT security objectives. Those responsible for the TOE must ensure that user authentication data is stored securely and not disclosed to unauthorized individuals. In particular:

a. Procedures must be established to ensure that user passwords generated by an administrator during user account creation or modification are distributed in a secure manner, as appropriate for the clearance of the system.

b. The media on which authentication data is stored must not be physically removable from the platform by unauthorized users.

c. Users must not disclose their passwords to other individuals.

d. Procedures must exist to assign appropriate clearances to users and sensitivity labels to objects. [CAPP][LSPP]

[O.E_BOOT] Hardware and firmware within the IT environment shall ensure that the correct copy of the Solaris 10 11/06 Operating System is “booted” during system start-up.

Note: The above applies to both workstations and servers. Administrators should also take precautions to prevent booting from the floppy drive, CD device or over the network where this is considered a threat.

[O.E_CONNECT] Those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets. [RBAC]

[O.E_CONSISTENCY] Administrators of the TOE must establish and implement procedures to ensure the consistency of the security-related data across all distributed components that are networked to form a single system (e.g. authentication data). In particular, if the product comprises more than one platform, all such platforms are administered from a central point within each LDAP domain.

[O.E_INSTALL] Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the networked product are distributed, installed and configured in a secure manner. [RBAC][CAPP][LSPP]

[O.E_INFO_PROTECT] Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

a. DAC protections on security critical files (such as audit trails and authentication databases) shall always be set up correctly.

b. All network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted.

c. If a system console is used, it must be connected directly to the machine, and must be afforded the same physical protections as the server or workstation. Access onto the system console is protected by user identification and authentication mechanisms. Access to its configuration is protected by a password.

d. Where applicable, the system controller must be connected directly to the server, and must be afforded the same physical protections as the server. The system controller will not be accessible via a network connection. Access onto the system controller is protected by a password.

[O.E_MAINTENANCE] Administrators of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.

[O.E_RECOVER] Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that, after system failure or other discontinuity, recovery without a protection (i.e., security) compromise is obtained.

[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 which might compromise IT security objectives. [RBAC][CAPP][LSPP]

[O.E_SOFTWARE_IN] Those responsible for the TOE shall ensure that the system shall be configured so that only an administrator can introduce new software into the system.

[O.E_SERIAL_LOGIN] Those responsible for the TOE shall implement procedures to ensure that users clear the screen before logging off where serial login devices(e.g. VT100) are used.

The following security objective applies in environments where specific threats to distributed systems need to be countered, as described in section 3. Typically this objective is met by cryptographic protection of network connections.

[O.E_PROTECT] Those responsible for the TOE must ensure that procedures and/or mechanisms exist to ensure that data transferred between platforms is secured from disclosure, interruption or tampering.

Security Requirements

5.1 TOE Security Functional Requirements

The Security Functional Requirements (SFRs) for the TOE are listed below in table 5-1 (classes, families, components and elements), with cross-references to [CAPP], [LSPP], and [RBAC] where these are derived from any PP.

The elements that are tailored for this security target are indicated by a * after the element's name in the table. These tailored elements are detailed in sub-section 5.1.1, below, with the new material underlined.

SFRs **in addition** to those taken from the [CAPP], [LSPP], and [RBAC] PPs for this security target are indicated in Table 5-1 with *italics*. These additional elements are conformant with Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.3, CCIMB-2005-08-002, August 2005[CCP2], and are detailed in Section 5.2, below. The remaining SFRs in the table are to be used for this ST exactly as they appear in [CAPP], [LSPP], and [RBAC].

Table 5-1 Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] para.	[LSPP] para.	[RBAC] para.	
FAU	FAU_GEN	FAU_GEN.1	FAU_GEN.1.1	5.1.1.1	5.1.1.1	5.1.1	
			FAU_GEN.1.2	5.1.1.2	5.1.1.2	5.1.1	
	FAU_SAR	FAU_SAR.1	FAU_SAR.1.1	5.1.3.1	5.1.3.1	5.1.1	
			FAU_SAR.1.2	5.1.3.2	5.1.3.2	5.1.1	
			FAU_SAR.2	5.1.4.1	5.1.4.1	5.1.1	
	FAU_SEL	FAU_SEL.1	FAU_SEL.1.1*	5.1.6.1	5.1.6.1	5.1.1	
			FAU_SEL.1.2*	5.1.6.1	5.1.6.1	5.1.1	
	FAU_STG	FAU_STG.1	FAU_STG.1	FAU_STG.1.1	5.1.7.1	5.1.7.1	5.1.1
				FAU_STG.1.2	5.1.7.2	5.1.7.2	5.1.1
		FAU_STG.3	FAU_STG.3	FAU_STG.3.1*	5.1.8.1	5.1.8.1	
FAU_STG.3.2*				5.1.8.1	5.1.8.1		
FAU_STG.4	FAU_STG.4	FAU_STG.4.1*	5.1.9.1	5.1.9.1			
		FAU_STG.4.2*	5.1.9.1	5.1.9.1			

Table 5-1 Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] para.	[LSP] para.	[RBAC] para.
FDP	FDP_ACC	FDP_ACC.1	FDP_ACC.1.1*	5.2.1.1	5.2.1.1	5.1.2
		FDP_ACF.1	FDP_ACF.1.1*	5.2.2.1	5.2.2.1	5.1.2
			FDP_ACF.1.2*	5.2.2.2	5.2.2.2	
			FDP_ACF.1.3*	5.2.2.3	5.2.2.3	
	FDP_ACF.1.4*		5.2.2.4	5.2.2.4		
	FDP_ETC	FDP_ETC.1	FDP_ETC.1.1		5.2.3.1	
			FDP_ETC.1.2		5.2.3.2	
			FDP_ETC.1.3*		5.2.3.3	
		FDP_ETC.2	FDP_ETC.2.1	5.2.4.1		
		FDP_ETC.2.2	5.2.4.2			
		FDP_ETC.2.3	5.2.4.3			
		FDP_ETC.2.4*	5.2.4.4			
	FDP_IFC	FDP_IFC.1	FDP_IFC.1.1*		5.2.5.1	
		FDP_IFF.2	FDP_IFF.2.1		5.2.6.1	
FDP_IFF.2.2			5.2.6.2			
FDP_IFF.2.3*			5.2.6.3			
FDP_IFF.2.4*			5.2.6.4			
FDP_IFF.2.5*			5.2.6.5			
FDP_IFF.2.6*			5.2.6.6			
FDP_IFF.2.7	5.2.6.7					
FDP_ITC	FDP_ITC.1	FDP_ITC.1.1		5.2.7.1		
		FDP_ITC.1.2		5.2.7.2		
		FDP_ITC.1.3*		5.2.7.3		
	FDP_ITC.2	FDP_ITC.2.1	5.2.8.1			
		FDP_ITC.2.2	5.2.8.2			
	FDP_ITC.2.3	5.2.8.3				
	FDP_ITC.2.4	5.2.8.4				
	FDP_ITC.2.5*	5.2.8.5				
FDP_RIP	FDP_RIP.2	FDP_RIP.2	5.2.3.1	5.2.9.1		
	FDP_RIP.2	FDP_RIP.2	5.2.4.1	5.2.10.1		
<i>FDP_UCT</i>	<i>FDP_UCT.1</i>	<i>FDP_UCT.1.1</i>	N/A	N/A	N/A	
<i>FDP_UIT</i>	<i>FDP_UIT.1</i>	<i>FDP_UIT.1.1</i> <i>FDP_UIT.1.2</i>	N/A	N/A	N/A	

Table 5-1 Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] para.	[LSPP] para.	[RBAC] para.
FIA	FIA_ATD	FIA_ATD.1	FIA_ATD.1.1*	5.3.1.1	5.3.1.1	5.1.3
	FIA_SOS	FIA_SOS.1	FIA_SOS.1.1	5.3.2.1	5.3.2.1	
	FIA_UAU	FIA_UAU.1	FIA_UAU.1.1*	5.3.3.1	5.3.3.1	
			FIA_UAU.1.2	5.3.3.2	5.3.3.2	
			FIA_UAU.2	FIA_UAU2.1		
	FIA_UID	FIA_UID.1	FIA_UID.1.1*	5.3.5.1	5.3.5.1	
			FIA_UID.1.2	5.3.5.2	5.3.5.2	
	FIA_USB	FIA_USB.1	FIA_USB.1.1*	5.3.6.1	5.3.6.1	5.1.3
				5.3.6.2	5.3.6.2	
				5.3.6.3	5.3.6.3	
FMT	FMT_MSA	FMT_MSA.1	FMT_MSA.1.1*	5.4.1.1	5.4.1.1	5.1.4
			FMT_MSA.1.1*		5.4.1.2	
			FMT_MSA.2.1			5.1.4
	FMT_MSA.3	FMT_MSA.3.1*	5.4.2.1	5.4.2.1	5.1.4	
			FMT_MSA.3.2*	5.4.2.2	5.4.2.3	5.1.4
	FMT_MTD	FMT_MTD.1	FMT_MTD.1.1	5.4.3	5.4.3	5.1.4
				5.4.4	5.4.4	
				5.4.5	5.4.5	
				5.4.6	5.4.6	
		FMT_MTD.3	FMT_MTD.3.1			5.1.4
FMT_REV	FMT_REV.1	FMT_REV.1.1	5.4.7.1	5.4.7.1	5.1.4	
			FMT_REV.1.2*	5.4.7.2	5.4.7.2	5.1.4
			FMT_REV.1.1	5.4.8.1	5.4.8.1	
			FMT_REV.1.2*	5.4.8.2	5.4.8.2	
FMT_SMR	FMT_SMR.1	FMT_SMR.1.1*	5.4.9.1	5.4.9.1		
			FMT_SMR.1.2	5.4.9.2	5.4.9.2	
	FMT_SMR.2	FMT_SMR.2.1*			5.1.4	
			FMT_SMR.2.2*		5.1.4	
			FMT_SMR.2.3*		5.1.4	
<i>FMT_SMF</i>	<i>FMT_SMF.1</i>	<i>FMT_SMF.1.1</i>				

Table 5-1 Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] para.	[LSPP] para.	[RBAC] para.
FPT	FPT_AMT	FPT_AMT.1	FPT_AMT.1.1*	5.5.1.1	5.5.1.1	5.1.5
	FPT_FLS	FPT_FLS.1	FPT_FLS.1.1			5.1.5
	FPT_RCV	FPT_RCV.1	FPT_RCV.1.1			5.1.5
			FPT_RCV.4	FPT_RCV.4.1*		
	FPT_RVM	FPT_RVM.1	FPT_RVM.1.1	5.5.2.1	5.5.2.1	5.1.5
	FPT_SEP	FPT_SEP.1	FPT_SEP.1.1	5.5.3.1	5.5.3.1	5.1.5
			FPT_SEP.1.2	5.5.3.2	5.5.3.2	5.1.5
	FPT_STM	FPT_STM.1	FPT_STM.1.1	5.5.4.1	5.5.4.1	5.1.5
FPT_TST	FPT_TST.1	FPT_TST.1.1			5.1.5	
		FPT_TST.1.2			5.1.5	
		FPT_TST.1.3			5.1.5	
FTA	FTA_LSA	FTA_LSA.1	FTA_LSA.1.1			5.1.6
	FTA_TSE	FTA_TSE.1	FTA_TSE.1.1			5.1.6
	<i>FTA_SSL</i>	<i>FTA_SSL.1</i>	<i>FTA_SSL.1.1</i>			
			<i>FTA_SSL.1.2</i>			
	<i>FTA_SSL.2</i>	<i>FTA_SSL.2.1</i>				
		<i>FTA_SSL.2.2</i>				
FTP	<i>FTP_ITC</i>	<i>FTP_ITC.1</i>	<i>FTP_ITC.1.1</i>			
			<i>FTP_ITC.1.2</i>			
			<i>FTP_ITC.1.2</i>			
	<i>FTP_TRP</i>	<i>FTP_TRP.1</i>	<i>FTP_TRP.1.1</i>			
			<i>FTP_TRP.1.2</i>			
			<i>FTP_TRP.1.3</i>			

5.1.1 Protection Profile SFRs Tailored for This ST

This sections contains the elements that correspond to the [RBAC], [CAPP], and [LSPP] Protection Profiles that are tailored for this security target (as indicated by a * after the element's name in Table 5-1, above) with the new material underlined. Note that [CAPP/LSPP] is indicated where both PPs share the SFR, though the [LSPP] version (and reference) is used for the purpose of completing operations since the [LSPP] is a superset of the [CAPP].

5.1.2 Security Audit (FAU)

[CAPP/LSPP] 5.1.5.1 The TSF shall provide the ability to perform searches of audit data based on the following attributes: FAU_SAR.3.1

- a. User identity;
- b. Subject sensitivity label;
- c. Object sensitivity label;
- d. type of audit event and audit class.

[CAPP/LSPP] 5.1.6.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: FAU_SEL.1.1

- a. User identity;
- b. Subject sensitivity label;
- c. Object sensitivity label;
- d. audit class.

[CAPP/LSPP] 5.1.8.1 The TSF shall generate an alarm to the authorized administrator if the audit trail exceeds or meets 100% occupancy. FAU_STG.3.1

Note: An alarm is generated once 100% of the allocated audit space is reached. This allocated space may be exceeded in certain circumstances e.g. by auditable actions taken by authorized administrators.

[CAPP/LSPP] 5.1.9.1 The TSF shall be able to prevent auditable events, except those taken by the authorized administrator, if the audit trail is full. FAU_STG.4.1

5.1.3 User Data Protection (FDP)

[CAPP/LSPP] 5.2.1.1 The TSF shall enforce the Discretionary Access Control Policy on processes acting on the behalf of users, filesystem objects and all operations among subjects and objects covered by the DAC policy. FDP_ACC.1.1

[CAPP/LSPP] 5.2.2.1 The TSF shall enforce the Discretionary Access Control Policy on objects based on the following: FDP_ACF.1.1

- a. The user identity and group membership(s) associated with a subject; and
- b. The access control attributes associated with an object: ACL, permission bits

[CAPP/LSPP] 5.2.2.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: FDP_ACF.1.2

IF the object has an explicit ACL, THEN:

- access granted to the object's owner is based on the user::rwx permissions
- access granted to individuals specified in the ACL is based on the bitwise AND operation of the user:[specified]:rwx and mask:rwx permissions
- access granted to subjects who belong to the object's group is based on the bitwise AND operation of the group::rwx and the mask:rwx entries
- access granted to subjects who belong to groups specified in the ACL is based on the bitwise AND operation of the group:[specified]:rwx and mask:rwx permissions
- access granted to all other subjects is based on the object's other permissions

ELSE

- access granted to the object's owner is based on the object user rwx permissions
- access granted to subjects who belong to the object's group is based on the object group rwx permissions
- access granted to all other subjects is based on the object other rwx permissions

[CAPP/LSP] 5.2.2.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rule: FDP_ACF.1.3

- a. If a subject has an effective override privilege, the TSF shall authorize access of the subject to any given filesystem object, even if such access is disallowed by FDP_ACF.1.2.

[CAPP/LSP] 5.2.2.4 The TSF shall explicitly deny access of subjects to objects based on no additional rules. FDP_ACF.1.4

[LSP] 5.2.3.3 The TSF shall enforce the following rules when unlabeled user data is exported from the TSC: FDP_ETC.1.2

- a) Devices used export data without security attributes cannot be used to export data with security attributes unless the change in device state is performed manually and is auditable;
- b) no additional exportation control rules.

[LSP] 5.2.4.4 The TSF shall enforce the following rules when labeled user data is exported from the TSC: FDP_ETC.2.5

- a) When data is exported in a human-readable or printable form: - The authorized administrator shall be able to specify the printable label which is assigned to the sensitivity label associated with the data. - Each print job shall be marked at the beginning and end with the printable label assigned to the 'least upper bound' sensitivity label of all the data exported in the print job. - Each page of printed output shall be marked with the printable label assigned to the 'least upper bound' sensitivity label of all the data exported to the page. By default this marking shall appear on both the top and bottom of each printed page.
- b) Devices used to export data with security attributes cannot be used to export data without security attributes unless the change in device state is performed manually and is auditable;

c) Devices used to export data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data;

d) no additional exportation control rules.

[LSPP] 5.2.5.1 The TSF shall enforce the Mandatory Access Control Policy on subjects, objects, and all operations among subjects and objects covered by the MAC policy.
FDP_IFC.1.1

[LSPP] 5.2.6.3 The TSF shall enforce the no additional information flow control SFP rules. FDP_IFF.2.3

[LSPP] 5.2.6.4 The TSF shall provide the following no additional SFP capabilities.
FDP_IFF.2.4

[LSPP] 5.2.6.5 The TSF shall explicitly authorize an information flow based on the following rules: if a subject has an appropriate override privilege, the TSF shall authorize the information flow, even if such access is disallowed by FDP_IFF.2.2. FDP_IFF.2.5

[LSPP] 5.2.6.6 The TSF shall explicitly deny an information flow based on the following rules: no additional rules. FDP_IFF.2.6

[LSPP] 5.2.7.3 The TSF shall enforce the following rules when importing unlabeled user data controlled under the MAC policy from outside the TSC: FDP_ITC.1.3

a) Devices used to import data without security attributes cannot be used to import data with security attributes unless the change in device state is performed manually and is auditable.

b) no additional importation control rules.

[LSPP] 5.2.8.5 The TSF shall enforce the following rules when importing labeled user data controlled under the MAC policy from outside the TSC: FDP_ACF.1.4

a) Devices used to import data with security attributes cannot be used to import data without security attributes unless the change in device state is performed manually and is auditable;

b) no additional importation control rules;

c) Sensitivity label, consisting of the following:

- A hierarchical level; and
- A set of non-hierarchical categories.

5.1.4 Identification and Authentication (FIA)

[CAPP/LSPP] 5.3.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: FIA_ATD.1.1

- a. User Identifier;
- b. Group Memberships;
- c. Authentication Data;

- d. User Clearances;
- e. Security-relevant Roles; and
- f. login shell.

[CAPP/LSP] 5.3.3.1 The TSF shall allow the following TSF-mediated actions on behalf of the user to be performed before the user is authenticated ^{FIA_UAU.1.1}

- a. select language;
- b. select desktop or console login;
- c. select remote host for login;
- d. help for login function.

[CAPP/LSP] 5.3.5.1 The TSF shall allow the following TSF-mediated actions on behalf of the user to be performed before the user is identified. ^{FIA_UID.1.1}

- a. select language;
- b. select desktop or console login;
- c. select remote host for login;
- d. help for login function.

[CAPP/LSP] 5.3.6.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: ^{FIA_USB.1.1}

- 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 sensitivity label used to enforce the Mandatory Access Control Policy, which consists of the following:
 - A hierarchical level; and
 - A set of non-hierarchical categories.
- e. upon successful identification and authentication, the real, effective and audit identities and real and effective group identifiers associated with the user identifier will be assigned to the resulting process executing on behalf of the user.

[CAPP/LSP] 5.3.6.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of a user: ^{FIA_USB.1.2}

- a. The sensitivity label associated with a subject shall be within the clearance range of the user;

- b. upon successful identification and authentication, the real, effective and audit identities, real and effective group identifiers, and sensitivity label associated with the user identifier will be assigned to the resulting process executing on behalf of the user

[CAPP/LSPP] 5.3.6.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of a user: ^{FIA_USB.1.3}

- a. The effective user identity associated with a subject can be changed to another user's identity via a command, provided that the effective user carried override privilege or successful authentication as the new user identity has been achieved;
- b. When executing a file which has the set UID permission bit set, the effective user identity associated with the subject shall be changed to that of the owner of the file;
- c. When executing a file which has the set GID permission bit set, the effective group identity associated with the subject shall be changed to that of the group attribute of the file.

Application Note: The DAC policy is enforced based on the effective UID as described above. All auditable events are recorded with the audit ID, which contains the identity of the user at identification time. In this manner, all auditable events can be traced back to the person initially identified to the TOE and are not associated to another person who may at some time identify them self as the alternate identity.

5.1.5 Security Management (FMT)

[CAPP/LSPP] 5.4.1.1 The TSF shall enforce the Discretionary Access Control Policy to restrict the ability to modify the access control attributes associated with a named object to the subject that owns the object and a subject with an effective override privilege. ^{FMT_MSA.1.1}

[LSPP] 5.4.1.2 The TSF shall enforce the Mandatory Access Control Policy to restrict the ability to modify the sensitivity label associated with an object to a subject that has mandatory and discretionary write access and possesses an appropriate privilege or authority. ^{FMT_MSA.1.1}

[RBAC] 5.1.4 The TSF shall enforce the RBAC SFP to provide restrictive default values for object security attributes that are used to enforce the SFP. ^{FMT_MSA.3.1}

[CAPP/LSPP] 5.4.2.3 The TSF shall allow the authorized administrators and users authorized by the Discretionary and Mandatory Access Control Policies to modify object security attributes to specify alternative initial values to override the default values when an object or information is created. ^{FMT_MSA.3.2}

[CAPP/LSPP] 5.4.7.2 The TSF shall enforce the rules: ^{FMT_REV.1.2}

- a. The immediate revocation of security-relevant authorizations; and
- b. when immediate revocation is not required by the authorized administrator, the user security attribute changes will become effective the next time the user logs in.

[CAPP/LSPP] 5.4.8.2 The TSF shall enforce the rules: ^{FMT_REV.1.2}

- 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. no additional rules.

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.

Rationale: This component supports the O.DISCRETIONARY ACCESS objective by providing that specified access control attributes are enforced at some fixed point in time.

5.1.6 Security Management Roles

[CAPP/LSP] 5.4.9.1 The TSF shall maintain the roles.^{FMT_SMR.1.1}

- a. Set of RBAC administrative roles;
- b. users authorized by the Discretionary Access Control Policy to modify object security attributes;
- c. users authorized by the Mandatory Access Control Policy to modify object security attributes;
- d. users authorized to modify their own authentication data;
- e. [RBAC] 5.1.4 Restrictions on Roles for the Object owner and administrator
FMT_SMR.2.1

[RBAC] 5.1.4 The TSF shall be able to associate users with roles.^{FMT_SMR.2.2}

The TSF shall ensure that the following conditions are satisfied:

- a. Object owners can modify security attributes for only the objects that they own;
- b. [RBAC] 5.1.4 The set of RBAC administrative roles can modify security attributes for all objects under the control of the TOE.^{FMT_SMR.2.3}

5.1.7 Protection of the TSF (FPT)

[CAPP/LSP] 5.5.1.1 The TSF shall run a suite of tests at the request of an authorized administrator to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.^{FPT_AMT.1.1}

5.1.8 Trusted Recovery

[RBAC] 5.1.5 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.1.1

The TSF shall ensure that the following SFs and failure scenarios have the property that the SF either completes successfully, or the indicated failure scenarios recovers to a consistent and secure state:

- a. The SF checks whether a specified privilege is assigned to any role but the database containing the privilege data is not on-line or the particular data table is inaccessible;
- b. [RBAC] 5.1.5 The SF checks whether a specified role has been assigned to a particular user but the database containing the role membership information is not on-line or the particular data table is inaccessible. FPT_RCV.4.1

5.1.9 Specification of Management Functions

[CEM-2] Note below: The TSF shall be capable of allowing the administrative user to perform the following management functions: FMT_SMF.1

- a. Object security attributes management
- b. Management of user accounts and roles (create, delete, modify)
- c. Authentication data management
- d. Management of security settings
- e. Audit administration

NOTE: This security functional requirement has been added as a result of AIS 32, Final Interpretation 065. The security functional requirement was added because a dependency from FMT_MSA.1 and FMT_MTD.1 to this new component has been defined in ASI 32, Final Interpretation 065.

5.1.10 TOE Access

[CEM-2] 501 The TSF shall lock an interactive session after an administrator-defined time interval of user activity by;

- clearing or overwriting display devices, making the current contents unreadable
- disabling any activity of the user's data access/display devices other than unlocking the session. FTA_SSL.1.1

The TSF shall require the following events to occur prior to unlocking the session: the user must be successfully re-authenticated. FTA_SSL.1.2

[CEM-2] 501 The TSF shall allow user-initiated locking of the user's own interactive session by;

- clearing or overwriting display devices, making the current contents unreadable
- disabling any activity of the user's data access/display devices other than unlocking the session. ^{FTA_SSL.2.1}

The TSF shall require the following events to occur prior to unlocking the session: the user must be successfully re-authenticated. ^{FTA_SSL.2.2}

5.2 Additional SFRs for This ST

This section contains the SFR elements (as indicated in *italics* in Table 5-1, above) included in this ST that are **in addition** to the requirements defined by either the [CAPP], [LSPP], or [RBAC] PP's.

5.2.1 Security Management (FMT)

5.2.1.1 Specification of Management Functions

[CCP2] *Note below:* The TSF shall be capable of performing the following security management functions: ^{FMT_SMF.1.1}

- a. Object security attributes management
- b. Management of user accounts and roles (create, delete, modify)
- c. Authentication data management
- d. Management of security settings
- e. Audit administration

Note: See application note at beginning of Section 5, above.

5.2.1.2 TOE Access (FTA)

Session Locking

[CCP2] The TSF shall lock an interactive session after an administrator-defined time interval of user activity by;

- a. clearing or overwriting display devices, making the current contents unreadable
- b. disabling any activity of the user's data access/display devices other than unlocking the session. ^{FTA_SSL.1.1}

The TSF shall require the following events to occur prior to unlocking the session:

- a. the user must be successfully re-authenticated. ^{FTA_SSL.1.2}

[CCP2] The TSF shall allow user-initiated locking of the user's own interactive session by;

- a. clearing or overwriting display devices, making the current contents unreadable
- b. disabling any activity of the user's data access/display devices other than unlocking the session. ^{FTA_SSL.2.1}

The TSF shall require the following events to occur prior to unlocking the session:

- a. the user must be successfully re-authenticated. ^{FTA_SSL.2.2}

5.2.2 User Data Protection (FDP)

5.2.2.1 Inter-TSF User Data Confidentiality Transfer Protection

[CCP2] The TSF shall enforce the Discretionary Access Control Policy to be able to transmit and receive objects in a manner protected from unauthorized disclosure. ^{FDP_UCT.1.1}

5.2.2.2 Inter-TSF User Data Integrity Transfer Protection

[CCP2] The TSF shall enforce the Discretionary Access Control Policy to be able to transmit and receive user data in a manner protected from modification and insertion errors. ^{FDP_UIT.1.1}

[CCP2] The TSF shall be able to determine on receipt of user data, whether modification or insertion has occurred. ^{FDP_UIT.1.2}

5.2.3 Trusted Path/Channels (FTP)

5.2.3.1 Inter-TSF Trusted Channel

[CCP2] The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. ^{FTP_ITC.1.1}

[CCP2] The TSF shall permit the TSF or the remote trusted IT product to initiate communication via the trusted channel. ^{FTP_ITC.1.2}

[CCP2] The TSF shall initiate communication via the trusted channel for, nfs (standard network filesystem access protocol), ftp (file transfer protocol), rcp (remote copy), rdist (remote file distribution), rlogin (remote login), rsh (remote shell), and telnet.

5.2.3.2 Trusted Path

[CCP2] The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. ^{FTP_TRP.1.1}

[CCP2] The TSF shall permit local and remote users to initiate communication via the trusted path. ^{FTP_TRP.1.2}

[CCP2] The TSF shall require the use of the trusted path for initial user authentication; user identification; changing of roles; changing of current group; changing of password and changing of sensitivity labels ^{FTP_TRP.1.3}

5.3 Strength of Function

The claimed minimum strength of function is *SOF-medium*.

5.4 TOE Security Assurance Requirements

The target evaluation assurance level for the product is EAL4+ [CC]. Assurance is augmented by ALC_FLR.3 Systematic Flaw Remediation.

5.5 Security Requirements for the IT Environment

The IT environment is required to meet the objectives described in Section 4.2. All but one of these objectives is met by procedural measures, however O.E_BOOT is met by either the OpenBoot PROM, System Controller, or x86/x64 PROM. Refinements to the CC Part 2 functional component are identified by emboldened text. The functionality provided by this firmware/SC is specified as follows:

5.5.1 OpenBoot PROM

The **platforms with OpenBoot PROM** shall restrict the ability to modify the behavior of the boot strapping process to users who know the valid PROM password.^{FMT_MOF.1.1:1}

Application Note: In fully secure and command-secure modes, the valid (booting) password is required in order to configure the PROM operating modes, passwords or boot parameters as required by the [SRN].

5.5.2 System Controller (SC)

The **platforms with a System Controller** shall restrict the ability to modify the behavior of the boot strapping process to users who know the valid SC password.^{FMT_MOF.1.1:2}

Application Note: A valid (booting) password is required in order to configure the SC operating modes, passwords or boot parameters as required by the [SRN].

5.5.3 x86/x64 Workstations and Servers

The **x86/x64 Workstations and Server platforms** shall restrict the ability to modify the behavior of the boot strapping process to users who know the valid PROM password.^{FMT_MOF.1.1:2}

Application Note: A valid (booting) password is required in order to configure the operating modes, passwords or boot parameters as required by the [SRN].

6.1 IT Security Functions

The ITSFs to which the claimed Strength of Function (SoF) rating applies are as follows:

- IA.1
- IA.11

6.1.1 Discretionary Access Control (DAC)

Policy

The security-related software shall define and control access between named users and named objects (e.g., files and programs) in the data processing system. All named users and named objects shall be uniquely identifiable over all the platforms in the system.

Within Trusted Extensions, DAC is applied in two different ways depending on the type of object. This ST therefore defines two object types:

- Objects that have permissions that can be changed by the owner;
- Objects that have permissions that are fixed or implicit given a process context.

The enforcement mechanisms for the former type of object shall allow users to specify and control sharing of those objects, initially generated by the user, by named users (group control is optional) using the specific designations of read, write, execute/search.

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

These access controls shall be capable of including or excluding access down to the level of a single user.

Access permission to these objects by users not already possessing access permission shall only be assigned by an authority responsible and authorized to grant access.

Subjects have a number of IDs associated with them:-

- effective user ID, real user ID, saved user ID;
- effective group ID, real group ID, saved group ID, supplemental groups; and

- audit user ID.

The Trusted Extensions discretionary access controls use the effective user ID and effective group ID for policing a subject's access rights over objects that have fixed or implicit permissions to within a process context.

Self/Group/Public/ACL Permissions

The product shall implement a discretionary access control mechanism that controls the access of subjects to named owner controlled objects. The discretionary access control mechanism shall associate with each object, an owner identification, a group identification, a set of access permissions and/or an access control list (ACL).

DAC.1 Subject to DAC.8, the access permissions on a filesystem object can be modified only by a subject that owns the object.

DAC.2 No subject may change the owner or group of an owner controlled object unless it is the owner of the object or has the following privilege effective:

- *priv_file_chown* - Allows a process to change a file's owner user ID. Also allows a process to change a file's group ID to one other than the process' effective group ID or one of the process' supplemental group IDs.

DAC.3 Subject to DAC.1, a subject may assign any combination of the following access modes to an owner controlled object:-

- read, write, execute/search
- to:-
- the owner of the object (self);
 - any member of the owning group (group); and
 - any user other than the owner or a member of the owning group (other).

DAC.4 Subject to DAC.1, an Access Control List (ACL) can be created for a *ufs* or *nfs* filesystem object to specify a set of allowable access modes (as per DAC.3) for individually named users or groups. If an ACL entry for a user or group contains no access modes, the specified user or group is specifically excluded from accessing the object. Users not listed anywhere in an ACL (either through explicit user ACL entries or through any applicable group ACL entries) shall have their access to the object determined by the "Other" ACL entry.

Note that the scope of the above Security Function is limited to regular files held on ufs and nfs filesystems. This includes hard links but excludes device special files, pipes and symbolic links. However, the regular files referenced by symbolic links can still be controlled by ACLs.

DAC.6 Whenever a subject requests access to an owner controlled object, the access permissions for that object shall be checked to determine whether the user who owns the subject can access the object in the requested mode. Where an ACL is defined for an object, it shall be used instead of the object's permission bits.

DAC.7 When a subject creates a filesystem object, the user ID of the subject is assigned to the object, and the user's umask restricts the initial access permissions of the object. The TOE default is that a user's umask is set to prevent any user other than the owner having write access to the object.

DAC.8 Subjects may only override discretionary access control if they have one or more of the following privileges effective;

- *priv_file_dac_execute*
- *priv_file_dac_read*
- *priv_file_dac_search*
- *priv_file_dac_write*
- *priv_file_owner*
- *priv_file_setid*
- *priv_ipc_dac_read*
- *priv_ipc_dac_write*
- *priv_ipc_owner*

DAC.9 The TSF shall enforce the Discretionary Access Control Policy to be able to transmit objects in a manner protected from unauthorized disclosure.

DAC.10 The TSF shall enforce the Discretionary Access Control Policy to be able to transmit and receive user data in a manner protected from modification and insertion errors.

6.1.2 Mandatory Access Control (MAC)

MAC.1 The security-related software shall define and control access between subjects and objects (e.g., files and programs) that contain data in the data processing system. All subjects and objects shall be uniquely identifiable over all the platforms in the system.

Trusted Extensions assigns sensitivity labels to all subjects (i.e., processes in the context of zones) and objects that can contain classified data, including file systems, devices, network endpoints and windows. The sensitivity labels consist of:

- a security level that represents the hierarchical relationships among subjects or objects; and
- classifications that can separate subjects or objects at the same security level.

MAC.2 When importing or exporting data or when interacting with the TOE the following rules apply:

- a. The security attributes of information imported from, or exported to a multi-level device are preserved by the import/export mechanism, and on export are stored on the same physical medium as the information itself.
- b. The TOE prints output surrounded by banner pages that contain the sensitivity label of the subject producing the output. Only users with the Print Without Banners authorization can print pages without banners.
- c. The banner pages include a statement warning that this output should be handled at the sensitivity level until it is manually reviewed and downgraded.
- d. Only users with the Print Without Labels authorization can print unlabeled pages to a multi-level printer.

- e. Only users with the Print a PostScript File authorization can print Post-Script documents to a multi-level printer. Note that it is possible to define multiple print queues and assign a single security level to each. This allows unlabeled printing (i.e., for PostScript documents) in a secure manner.
- f. Except when entering passwords (including login, re-authentication and password change), all local users can access the TOE via labeled windows only.
- g. Users are able to view the sensitivity label of each window at any time, if configured for that user, except when entering passwords.

MAC.3 The following are the basic MAC access control rules:

- a. Subject to (c), a subject can read (or execute or search) an object only if the subject's sensitivity label dominates the object's sensitivity label.
- b. Subject to (c), a subject can write to an object only if the object's sensitivity label equals the subject's sensitivity label. If the object is being created, the sensitivity label of the object shall equal the sensitivity label of the creating subject.
- c. A subject may override MAC checks, if and only if it has one or more of the following privileges effective. In order for a privilege to be effective for a subject in a zone other than the Global Zone, it must be effective for the subject and also the zone must be assigned that privilege.
 - *net_mac_aware* (to request a read-down mount, must be used in conjunction with the *sys_mount* privilege)
 - *net_bindmlp* (to bind a multi-level port)
 - *proc_zone* (to be aware of processes in other zones)
 - *win_mac_read* (to read non-dominated windows resources)
 - *win_mac_write* (to modify dominated windows resources)

MAC.4 The following rules represent constraints on subject sensitivity labels:

- a. If the subject is a normal user's subject, the subject's labels are bound by the user's label range. A user's label range consists of all the valid labels that dominate the user's minimum label and are dominated by the user's clearance. Valid labels and clearances are defined by the site in `label_encodings(4)`
- b. If the subject is a system subject (or role), the subject's labels are bound by `admin_low` and `admin_high`.
- c. A subject's label is determined by the label of the zone containing the subject. Only system subjects are permitted in the Global zone. System subjects with all privileges may change their SLs by entering a differently labeled zone.

MAC.5 The following rules represent constraints on object sensitivity labels:

A subject can set the sensitivity label of objects to which it has mandatory and discretionary write access, only if it has one or more of the following privileges effective:

- *file_upgrade_sl* (to upgrade a file sensitivity label, i.e., move it to another zone)
- *file_downgrade_sl* (to downgrade a file sensitivity label, i.e., move it to another zone)
- *win_upgrade_sl* (to upgrade a window resource sensitivity label)
- *win_downgrade_sl* (to downgrade a window resource sensitivity label)

Devices in Unix are accessed as if they are file objects, and hence the MAC mediation rules given in section 5 define the policy that is assumed when subjects attempt to read or write information to/from devices.

Administrative users can create both single and multi-level devices. Trusted Extensions implements an allocation mechanism that allows normal users to use a device in single-level mode. If a device is not specified by an administrative user as an allocatable device, it will only act in multi-level mode.

MAC.6 The following rules represent constraints on devices:

- a. Only administrative users can specify a device as allocatable, set or change the sensitivity label range of a device, and specify which of the following categories of users may allocate the device:
 - users with the authorizations specified;
 - all users; and
 - no users.

Users with the Allocate Device authorization will have access to single level allocatable devices. For these devices the following rule applies:

- b. A user may only import or export data to a single-level device if the device is allocated to that user, and the user's subject has a sensitivity label that is within the sensitivity label range of the device. The data shall be imported or exported at the sensitivity label of the user's subject.

When exporting data to a single-level device, data can only be written to the device by subjects which are dominated by the sensitivity label of the device. As these subjects can only read data that they dominate, only data dominated by the sensitivity label of the device can be written to it.

MAC.7 The following rules represent constraints on windows:

- a. The sensitivity label of a window must always be dominated by the sensitivity label of the user logged in at the device on which the window is displayed and must always be contained within the device sensitivity label range of the device on which the window is displayed.
- b. When a process that does not have the *win_selection* privilege requests an inter-window data move from one window to another that does not have the same sensitivity label, the product shall ensure that the user is notified that the windows have different sensitivity labels before allowing the move.

- c. In order to perform an inter-window move when the sensitivity label of the data being moved is not dominated by ('is higher than') the sensitivity label of the destination to which the data is being moved, the user must possess the Paste to a Downgraded Window authorization.
- d. In order to perform an inter-window move when the sensitivity label of the data being moved is dominated by ('is lower than') the sensitivity label of the destination to which the data is being moved, the user must possess the Paste to a Upgraded Window authorization.

MAC.8 The following rules represent constraints on networks:

- a. The sensitivity label of data transmitted over the network between hosts shall be within the sensitivity label range, as configured by the authorized administrator, of:
 - the local host sending the data;
 - the local network interface used to send the data;
 - the remote host receiving the data; and
 - the remote network interface used to receive the data.

The sensitivity label range of a network interface can be set to be a single label by setting the minimum and maximum sensitivity labels to the same level. This constrains all data sent and received over the interface to be at this single label, creating a single-level network.

Unlabeled hosts are configured by placing them on a single-level network of the appropriate sensitivity label, and configuring the Trusted Extensions hosts to communicate with them using unlabeled packets.

- b. Data being transmitted over the local area network between workstations of the distributed product shall be labeled with the sensitivity label of the subject transmitting the data.

MAC.9 Unlabeled communications over the local area network are restricted to:

- communications between an unlabeled host and either a labeled or unlabeled host; and
- subjects on a labeled host that have the *net_rawaccess* privileges effective.

6.1.3 Object Reuse

OR.1 When an object is initially assigned, allocated or reallocated to a subject from the system's pool of unused objects, the security-related software shall assure that the object contains no data for which the subject is not authorized.

OR.2 When memory objects are allocated for use by a subject at run-time, the memory shall contain no data from a previous subject.

Any portion of a file object that has not been previously written to shall either:

- not be readable by any subject; or
- shall be cleared before it can be read.

OR.3 The TOE shall revoke all access rights held by a subject to the information contained within a storage object, before reuse by other subjects.

6.1.4 Identification and Authentication

Password Authentication

IA.1 The product shall require users to identify and successfully authenticate themselves, using a user name and a password, before performing any other actions.

IA.2 Upon successful identification and authentication, the real and audit user IDs and the real group IDs, clearances and authorizations of the user's subjects shall be those specified by the authentication data.

IA.3 Subject to IA.4, user accounts shall be unlocked by an administrative user only.

IA.4 The maximum number of failed login attempts shall be configured by an administrative user only. If the limit is reached, the user account shall be locked.

Password Generation and Selection

IA.5 Users shall be required to change their passwords within a specific frequency determined by an administrative user.

It should be noted that this SF does not preclude users from changing their passwords more frequently than required.

IA.6 If enabled by an administrative user, the product shall automatically notify users that their password must be changed.

Passwords shall be assigned by an administrative user or chosen by the users themselves.

IA.8 The product enforces a minimum user password length (except for PROM passwords), as specified in the `/etc/default/passwd` file.

Password Protection

The authentication data shall not contain a clear text version of each user's password, but rather a one-way encrypted value based on the user's password. When a user enters his password, it is used to construct an encrypted value and is compared against the encrypted value in the authentication data.

IA.9 On entry, passwords shall not be displayed in cleartext.

IA.10 User passwords are always stored in encrypted form.

Note: This SF does not apply to BOOTPROM or System Controller passwords (which are not user passwords, and are beyond the scope of this ST).

IA.11 The authentication data shall be protected so that it cannot be written other than as follows:

- by administrative users who may
 - create, delete user identities,
 - modify the name, primary group, secondary group, login shell;
 - set passwords if required;
 - modify the minimum login label, user clearance, user label view, user label visibility; and

- by a user supplying a new password, or a password being generated by the TOE, depending on the configuration of the TOE.

Note: In respect of [CAPP_5.4.7.2] requirements; The administrator can use the Administration tools to revoke access rights, security relevant authorizations and forcibly log off users if required.

IA.12 A workstation shall have the capability to identify positively other workstations of the distributed product before allowing them to be used for accessing system resources at that workstation.

IA.13 Only users with *Remote Login* authorizations may remotely login

6.1.5 Session Locking

SL.1 The TSF shall lock an interactive session after an administrator-defined time interval of user activity by clearing or overwriting display devices, making the current contents unreadable and disabling any activity of the user's data access/display devices other than unlocking the session.

SL.2 The TSF shall require that prior to unlocking an interactive session the user must be successfully re-authenticated.

SL.3 The TSF shall allow user-initiated locking of the user's own interactive session by clearing or overwriting display devices, making the current contents unreadable and disabling any activity of the user's data access/display devices other than unlocking the session.

SL.4 The TSF shall require that prior to unlocking a user's interactive session, the user must be successfully re-authenticated.

6.1.6 Secure Communication

The TOE provides the ability to protect communication against disclosure and undetected unauthorized modification.

SC.7 Communication channels provided by the TSF between itself and a remote trusted IT product must be logically distinct from other communications channels.

SC.8 The TSF must provide assured identification of the end points and protection of the channel data from modification or disclosure for communication channels provided by the TSF between itself and a remote trusted IT product.

SC.9 Communication channels provided by the TSF between itself and remote or local users are kept logically distinct from other communications channels through the use of encryption services that use specific session keys for each user/session.

6.1.7 Trusted Path

The security-related software shall support a direct trusted communication path, known as the trusted path, between itself and users for use when a positive connection between a user and the security-related software (TOE) is required (e.g., identification and authentication, change subject security label).

TPath.1 Communications between the trusted path shall be initiated exclusively by a user or the security-related software and shall be logically isolated and unmistakably distinguishable from other communications paths.

TPath.2 After a successful login, the trusted path shall be controlled by the product, which shall:

- provide for reserved portions of the screen to which user subjects cannot write;
- read all user input to determine whether the user is attempting to communicate via the trusted path; and,
- use a reserved portion of the screen to provide the user with visual confirmation that the current user input is via the trusted path.

TPath.3 The product shall use the trusted path mechanisms to allow the user to perform security-critical functions via the trusted path including, as a minimum:

- user identification;
- all operations that require users to enter passwords (e.g., authentication, change password);
- all operations that set sensitivity labels;
- allocation/deallocation of devices; and,
- all use of the actions or commands for the administration roles.

6.1.8 Administration

Profiles

Trusted Extensions provides the ability for an administrator to define profiles and assign profiles to users. Profiles are a powerful mechanism that allow administrators to define the commands and CDE actions that users are allowed to perform, together with the authorizations that the user has. This mechanism provides fine-grain control over user-capabilities and allows the system to rigorously implement the principle of least privilege.

Admin.1 Only administrators may assign a user profile to a user. The profile shall include:

- A list of desktop actions that the user is allowed to perform, and for each action:
 - The privilege that the action shall be performed with;
 - The real and effective user ID and the real and effective group ID that the action shall be performed with.
- A list of commands that the user is allowed to perform, and for each command:
 - The privileges that the command shall be executed with;
 - The real and effective user ID and the real and effective group ID that the command shall be executed with.
- A list of authorizations that shall be granted to the users assigned this profile.

Admin.2 Users may perform only those desktop actions as specified in their profiles, and when executed they are executed with the security attributes as specified by Admin.1.

Admin.3 Users who are configured to use the profile shell may execute only those commands as specified in their profiles, and when executed they are executed with the security attributes as specified by Admin.1.

Roles

Roles are configurable with Trusted Extensions, allowing the system to be configured so that the principle of least-privilege can be optimally implemented for each installation and application

The following rules apply to the configuration of roles:

Admin.4 Only an authorized user can define and assign roles to users.

Admin.5 The TSF shall restrict the scope of a session based on the role assigned to the user.

6.1.9 Audit

Audit Events

Audit.1 The use of the identification and authentication mechanisms is auditable. The following information is recorded for each event audited:-

- date;
- time;
- user identity - audit ID and effective user ID (if successful);
- security attributes of the user (if successful)
- identification of the server/workstation or terminal used; and
- success or failure of the event.

Audit.2 Attempts to access to objects are auditable. The following information is recorded for each event audited:-

- date;
- time;
- user identity - audit ID and effective user ID;
- sensitivity label of the user identity;
- name of the object;
- sensitivity label of the object;
- type of access attempted; and
- success or failure of the attempt.

Audit.3 The creation of an object is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- name of the object;
- sensitivity label of the object; and
- sensitivity label of creating subject.

Audit.4 The creation of a subject to run on behalf of a user is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- sensitivity label of the user;
- success or failure of the attempt;

Audit.5 The creation, deletion, disabling or enabling of user accounts is auditable. The following information is recorded for each event audited:

- date;
- time;
- identity of the user implementing the change - audit ID and effective user ID;
- sensitivity label of user implementing the change;
- name of the user account being modified; and
- type of action.

Audit.6 Attempts to assign or modify security attributes are auditable. The following information is recorded for each event audited:

- date;
- time;
- identity of the user implementing the change - audit ID and effective user ID;
- sensitivity label of user implementing the change;
- name of the user account or object being modified;
- type of attribute; and
- success or failure of the attempt.

Audit.7 The use of DAC override privileges are auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- sensitivity label of user identity;
- name of the object involved (if any);
- sensitivity label of the object involved (if any); and
- the privilege or role granted.

Audit.8 Security relevant events affecting the operation of the auditing functions are auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity (if relevant) - audit ID and effective user ID; and
- type of event.
- the privilege or role granted
-

Audit.9 Import or export of data to a device is auditable. The following information is recorded for each event audited;

- date;
- time;
- user identity - audit ID;
- sensitivity label of data to be imported or exported;

- sensitivity label of user identity;
- name of the object and device.

Audit.10 The creation or deletion of a logical device for storage media is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity (if relevant) - audit ID and effective user ID;
- sensitivity label of user identity;
- name of the object and device;
- sensitivity label of the object and device; and
- type of action.

Audit.11 Start-up and shutdown of the system is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity (mandatory for shutdown only) - audit ID and effective user ID; and
- type of event.

Audit.12 The date and time information recorded in audit records shall be reliable.

Audit.13 Applications can enter their own audit records into the system audit trail, if and only if the subject has either *proc_audit_appl* or *proc_audit_tcb* privileges effective.

Protection of Audit Information

Audit.14 Audit data shall be protected so that access to it is limited to administrative users.

Audit.15 Password data (in clear or encrypted form) is never recorded in the audit log.

Selective Audit Data Collection/Reduction

Audit.16 Only administrative users may define classes of audit event.

Audit.17 Only administrative users shall be able to define the default system audit-mask that defines which audit classes are recorded by default.

Audit.18 Only administrative users shall be able to define a per-user audit-mask that defines which audit classes are recorded for that user. For a given user, the system shall audit those classes that are in the default system audit mask or the per-user audit mask.

Audit.19 Audit reduction software shall be available to allow administrative users to selectively retrieve audit data based on, at a minimum, the identity of users, the type of audit event, and the audit class.

Audit Data Storage

Audit.20 Each server/workstation of the (distributed) product may store audit data locally or on another server/workstation of the product that can act as an audit server.

Audit.21 If another server/workstation of the product is being used as an audit server, and this audit server becomes unavailable, the (local) server/workstation shall either:

- automatically switch over to storing audit data locally,
- or
- suspend operation until the audit server is again available,
- or
- suspend operation until an alternative server/workstation of the product takes over as an audit server;
- or
- if no server/workstation is able to store audit data then no further auditable events shall occur (i.e., all auditable actions will be suspended).

Audit.22 Facilities are available to allow administrative users to archive and maintain the audit logs. Only such users may use these facilities to archive and maintain the audit logs.

Audit.23 The system shall notify an administrator of audit trail saturation.

6.1.10 Enforcement Functions

ENF.1 The TOE shall validate all actions between subjects and objects that require policy enforcement, before allowing the action to succeed.

ENF.2 The TOE shall maintain a domain 'kernel space' for its own trusted execution. This shall be kept separate from untrusted subjects which operate in a separate domain 'user space'.

ENF.3 The TOE shall allow an administrator to perform a self test to ensure that the underlying TSF is enforcing process separation.

ENF.4 The TSF shall ensure that only secure values are accepted for user passwords.

6.1.11 Failure

FAIL.1 After a failure or system discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FAIL.2 The TSF shall preserve a secure state when failures occur in the databases containing user privileges information or the functions related to user roles and privileges.

6.2 Required Security Mechanisms

6.2.1 Identification and Authentication

The TOE uses a username and password mechanism to provide authentication of users. The construction of passwords is sufficient to meet the requirements of a strength of function of Medium. This mechanism supports the IT SFs IA.1 and IA.11.

Passwords are encrypted using a proprietary one way hashing algorithm, however the assessment of algorithmic strength does not form part of the evaluation.

6.3 Assurance Measures

Assurance measures will be adopted to address each of the EAL4+ assurance requirements, as summarized in Table B.1 in [CC, Part 3] and as summarized below.

Table 6-1 How Assurance Requirements Will Be Met

Assurance components	Assurance Measure
ACM_AUT.1 Partial CM automation	Information on the automated CM tools will be provided in the Software Development Framework document.
ACM_CAP.4 Generation support and acceptance procedures	Configuration Management procedures will be provided for Trusted Extensions.
ACM_SCP.2 Problem tracking CM coverage	As for ACM_CAP.4.
ADO_DEL.2 Detection of modification	Delivery procedures will be provided for Trusted Extensions.
ADO_IGS.1 Installation, generation, and start-up procedures	Installation, generation and start-up procedures will be provided for Trusted Extensions.
ADV_FSP.2 Fully defined external interfaces	The Trusted Extensions MAN pages, which are relevant to the implementation of the security functions, will be provided to the evaluation and assessed against this assurance requirement.
ADV_HLD.2 Security enforcing high-level design	High-level Design will be provided for Trusted Extensions.
ADV_IMP.1 Subset of the implementation of the TSF	The source code for Trusted Extensions will be provided to the evaluation.
ADV_LLD.1 Descriptive low-level design	Low-level Design will be provided for Trusted Extensions.
ADV_RCR.1 Informal correspondence demonstration	This correspondence information will be contained in the functional specification and design documents. The functional specification will map SFs to MAN pages. The HLD will map ITSFs to the HLD, and the LLD will map ITSFs and source code modules to the LLD basic components.
ADV_SPM.1 Informal TOE security policy model	A separate Informal Security Policy Model (ISPM) will be provided to the evaluation.
AGD_ADM.1 Administrator guidance	The Trusted Extensions operational documentation relevant to an administrator will be provided.
AGD_USR.1 User guidance	The Trusted Extensions operational documentation relevant to an end user will be provided.

Assurance components	Assurance Measure
ALC_DVS.1 Identification of security measures	Development security documentation will be provided for Trusted Extensions.
ALC_FLR.3 Life Cycle Support	Flaw remediation procedures are in place for Trusted Extensions, documents and other evidence will be provided.
ALC_LCD.1 Developer defined life-cycle model	The Life Cycle definition for Trusted Extensions is documented in the Software Development Framework document.
ALC_TAT.1 Well-defined development tools	The tools used in the development of Trusted Extensions are the same as for Solaris 10 3/05 (the Solaris 10 11/06 and Trusted Extensions co-release followed Solaris 10 3/05).
ATE_COV.2 Analysis of coverage	The analysis of test coverage will be presented to the evaluation in a form similar to that provided to the Solaris 10 11/06 evaluation. The existing coverage is against both High and Low level designs and should therefore be to a sufficient depth.
ATE_DPT.1 Testing: high-level design	The analysis of test depth will be presented to the evaluation in a form similar to that provided to the Solaris 10 11/06 evaluation. The existing coverage is against both High and Low level designs and should therefore be to a sufficient depth.
ATE_FUN.1 Functional testing	The test documentation provided to the evaluation will be in a format similar to that provided to the Solaris 10 11/06 evaluation. The tests will be run on a range of platforms as specified in section 2.3.1.1
ATE_IND.2 Independent testing - sample	Access will be provided to the TOE in its evaluated configuration on an appropriate set of platforms, together with all resources needed to repeat the developer's tests
AVA_MSU.2 Validation of analysis	The Misuse Analysis previously submitted for the EAL4 evaluation of Solaris 10 11/06 will be updated for Trusted Extensions.
AVA_SOF.1 Strength of TOE security function evaluation	The Strength of Function analysis previously submitted for the EAL4 evaluation of Solaris 10 11/06 will be updated for Trusted Extensions.
AVA_VLA.2 Independent vulnerability analysis	The Developer Vulnerability Analysis previously submitted for the EAL4 evaluation of Solaris 10 11/06 will be updated for Trusted Extensions and submitted to fulfill this requirement. In addition, evidence of Sun's continuing search for vulnerabilities and the resolution of them in the Solaris product, will be provided.

This Page Intentionally Left Blank

This chapter presents the evidence used in the ST evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. The rationale also demonstrates that any PP conformance claims are valid.

7.1 Correlation of Threats, Policies, Assumptions and Objectives.

The correlation between threats, organizational policies, assumptions and objectives is detailed in the following sections, and is summarized below

Table 7-1 Mapping of Objectives to Threats and Organizational Policies

Objective	Threat and Policies
O.AUTHORIZATION	T.ACCESS_INFO, T.ACCESS_TOE, T.MODIFY, T.ADMIN_RIGHTS, P.AUTH, P.ACCOUNTABLE
O.ENTRY	T.ACCESS_INFO, T.ACCESS_TOE
O.DISCRETIONARY_ACCESS	T.ACCESS_INFO, T.MODIFY, P.DAC, P.NEED_TO_KNOW
O.MANDATORY_ACCESS	P.MAC
O.KNOWN	T.ACCESS_INFO, T.ACCESS_TOE, T.MODIFY, T.ADMIN_RIGHTS
O.AUDITING	T.ACCESS_INFO, T.ACCESS_TOE, T.MODIFY, P.ACCOUNTABLE, T.ADMIN_RIGHTS
O.ACCOUNT	T.ACCESS_INFO, T.ACCESS_TOE, T.MODIFY, T.ADMIN_RIGHTS, P.ACCOUNTABLE
O.TRUSTPATH	T.COMPROMISE, P.NEED_TO_KNOW
O.RESIDUAL_INFO	T.ACCESS_INFO, P.DAC, P.MAC, P.NEED_TO_KNOW
O.MANAGE	T.ACCESS_INFO, T.ACCESS_TOE, T.MODIFY, T.ADMIN_RIGHTS, P.AUTH, P.DAC, P.MAC, P.ACCOUNTABLE, P.NEED_TO_KNOW

Table 7-1 Mapping of Objectives to Threats and Organizational Policies

Objective	Threat and Policies
O.ENFORCEMENT	T.ACCESS_INFO, T.ACCESS_TOE, T.MODIFY, T.ADMIN_RIGHTS, P.AUTH, P.DAC, P.MAC, P.ACCOUNTABLE, P.NEED_TO_KNOW
O.DUTY	T.MODIFY, T.ADMIN_RIGHTS
O.HIERARCHICAL	T.ADMIN_RIGHTS
O.ROLE	T.ACCESS_INFO, T.MODIFY, T.ADMIN_RIGHTS

Table 7-2 Mapping of Threats to Objectives

Threat	Objective
T.ACCESS_INFO	O.AUTHORIZATION, O.ENTRY, O.DISCRETIONARY_ACCESS, O.KNOWN, O.ROLE, O.AUDITING, O.ACCOUNT, O.RESIDUAL_INFO, O.MANAGE, O.ENFORCEMENT
T.ACCESS_TOE	O.AUTHORIZATION, O.ENTRY, O.KNOWN, O.AUDITING, O.ACCOUNT, O.MANAGE, O.ENFORCEMENT
T.MODIFY	O.AUTHORIZATION, O.DISCRETIONARY_ACCESS, O.KNOWN, O.ROLE, O.AUDITING, O.ACCOUNT, O.MANAGE, O.ENFORCEMENT, O.DUTY
T.ADMIN_RIGHTS	O.AUTHORIZATION, O.KNOWN, O.ROLE, O.ACCOUNT, O.MANAGE, O.ENFORCEMENT, O.DUTY, O.HIERARCHICAL, O.AUDITING
T.COMPROMISE	O.TRUSTPATH
T.TRANSIT	O.E_INSTALL, O.E_INFO_PROTECT, O.E_PROTECT
T.OPERATE	O.E_ADMIN, O.E_ACCOUNTABLE, O.E_CREDEN, O.E_CONNECT, O.E_CONSISTENCY, O.E_PHYSICAL
T.ROLEDEV	O.E_ACCOUNTABLE, O.E_CONNECT, O.E_CONSISTENCY, O.E_CREDEN

Table 7-3 Mapping of Policies to Objectives

Policy	Objective
P.AUTH	O.AUTHORIZATION, O.MANAGE, O.ENFORCEMENT
P.DAC	O.DISCRETIONARY_ACCESS, O.RESIDUAL_INFO, O.ENFORCEMENT, O.MANAGE
P.MAC	O.MANDATORY_ACCESS, O.RESIDUAL_INFO, O.ENFORCEMENT, O.MANAGE
P.ACCOUNTABLE	O.AUDITING, O.AUTHORIZATION, O.MANAGE, O.ACCOUNT, O.ENFORCEMENT
P.NEED_TO_KNOW	O.DISCRETIONARY_ACCESS, O.RESIDUAL_INFO, O.ENFORCEMENT, O.MANAGE, O.TRUSTPATH

Table 7-4 Mapping of Objectives for the Environment to Threats, Assumptions and Policies

Objective	Threats and Assumptions
O.E_ADMIN	T.OPERATE, A.MANAGE, A.PASSWORD, A.NO_EVIL_ADM
O.E_ACCOUNTABLE	T.OPERATE, T.ROLEDEV, A.USER, A.MANAGE, A.ACCESS
O.E_AUDITDATA	A.MANAGE
O.E_CREDEN	T.OPERATE, T.ROLEDEV, A.USER, A.MANAGE, A.COOP, A.CLEARANCE, A.SENSITIVITY
O.E_BOOT	A.MANAGE
O.E_CONNECT	T.OPERATE, T.ROLEDEV, A.PROTECT, A.ASSET, A.MANAGE
O.E_CONSISTENCY	T.OPERATE, T.ROLEDEV, A.LDAP_DOMAINS, A.MANAGE, A.CONNECT
O.E_INSTALL	T.TRANSIT, A.PASSWORD, A.MANAGE, A.PEER, A.NO_EVIL_ADM
O.E_INFO_PROTECT	T.TRANSIT, A.PROTECT, A.ASSET, A.BRIDGES&ROUTERS, A.MANAGE
O.E_MAINTENANCE	A.MANAGE
O.E_RECOVER	A.MANAGE
O.E_PHYSICAL	T.OPERATE, A.LOCATE, A.MANAGE, A.CONNECT

Table 7-4 Mapping of Objectives for the Environment to Threats, Assumptions and Policies

Objective	Threats and Assumptions
O.E_SOFTWARE_IN	A.MANAGE
O.E_SERIAL_LOGIN	A.MANAGE, A.CONNECT
O.E_PROTECT	T.TRANSIT, A.PROTECT, A.ASSET, A.BRIDGES&ROUTERS, A.MANAGE, A.CONNECT

The OSPs are derived from the [CAPP], [LSPP], and [RBAC] and are included to indicate how the OSPs relate to the TOE security objectives and the primary non-IT security objectives. The OSPs are generally more abstract than the threats and so the correlation between similar threats and OSPs to objectives is not necessarily the same.

The environmental objectives O.E_ADMIN, O.E_BOOT, O.E_INSTALL and O.E_CONSISTENCY are general objectives which help counter all the threats (with the exception of T.TRANSIT in some cases) as follows:

[O.E_ADMIN] Those responsible for administering the TOE must be competent and trustworthy in order to manage the security functions effectively. Effective management is necessary in order that the threats are not inadvertently or deliberately realized;

[O.E_BOOT] and **[O.E_INSTALL]** ensure that the correct copy of the operating system is installed and subsequently booted in a secure manner, and is hence relevant to help counter all the threats;

[O.E_CONSISTENCY] is required to ensure that data is set up and maintained in a consistent manner across all platforms in the distributed system. Erroneous or duplicate entries in the authentication information may allow any of the threats to be realized.

7.2 Security Objectives Rationale

This section demonstrates that the security objectives stated in Section 4 above are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

7.2.1 Complete Coverage - Threats

This section provides evidence demonstrating coverage of the threats by both the IT and Non-IT security objectives.

[T.ACCESS_INFO] *An authorized user of the TOE accesses information without having permission from the person who owns, or is responsible for, the information.*

Security objectives O.DISCRETIONARY_ACCESS and O.ROLE counter this threat directly by ensuring the means are provided by which users can securely implement compartmentalization of information in order to counter this threat.

O.RESIDUAL_INFO helps counter the threat by ensuring that once an object has passed outside the control of DAC, that residual information contained in it is not passed to other users.

Security objectives O.AUTHORIZATION and O.KNOWN support O.DISCRETIONARY_ACCESS and O.ROLE in countering this threat by ensuring that an authorized user cannot impersonate another authorized user, thereby undermining the intent of O.DISCRETIONARY_ACCESS.

O.AUDITING helps counter this threat by ensuring that repeated [unsuccessful] attempts to access information to which the user is not granted permission, can be detected, thereby allowing the administrator to take action before the attack is successful. O.ACCOUNT states that the TOE must ensure that all users can be held accountable for their security relevant actions.

O.ENTRY which states that the TOE must prevent logical entry to it by persons or processes with no rights to access it.

O.MANAGE and O.ENFORCEMENT counter this threat by ensuring:

- privileged actions are controlled; and
- the access controls cannot be bypassed.

Support is also provided by the following security objectives for the environment:

- a.O.E_ADMIN - to administer the controls over access to information;
- b.O.E_BOOT - to ensure that information cannot be accessed by booting an alternative operating system;
- c.O.E_CREDEEN is required to protect the information which would otherwise enable attackers to gain access to the TOE;
- d.O.E_PROTECT - to ensure that data transmitted over network cabling is appropriately protected;
- e.O.E_RECOVER - to ensure that information cannot be accessed by terminating the operation of a server/workstation (whether intentional or not); and
- f.O.E_SERIAL_LOGIN - to ensure that information is not seen by users who do not have a need to know when serial devices are being used.
- g.O.E_PHYSICAL which states that those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.

[T.ACCESS_TOE] *An unauthorized user of the TOE gains access to the system, thereby gaining unauthorized access to information.*

O.AUTHORIZATION ensures that all users identify themselves to the system, and that their claimed identity is authenticated before being granted access to the system. This therefore prevents unauthorized users gaining access to the system. O.KNOWN also states that legitimate users of the system must be identified before rights of access can be granted.

O.AUDITING provides support in the form of auditing attempts to access the TOE. The auditing of unsuccessful attempts to login help to detect and hence counter the threat of repeated attacks on the access functions. O.ACCOUNT states that the TOE must ensure that all users can be held accountable for their security relevant actions.

O.ENTRY which states that the TOE must prevent logical entry to it by persons or processes with no rights to access it.

O.MANAGE and O.ENFORCEMENT support this threat by ensuring:

- the database of authorized users is properly managed and maintained;
- the authorization functions are always invoked and cannot be bypassed;
- the auditing functions are set up appropriately to detect repeated attempts to login.

Support is also provided by the following security objectives for the environment:

a.O.E_ADMIN - to ensure that the introduction of new user identities is a restricted operation and performed only by the users responsible.

b.O.E_ACCOUNTABLE - to ensure that unauthorized users are not provided with accounts enabling them to access the TOE;

c.O.E_CREDEN - which ensures that bad passwords, which might be used to determine valid passwords, are not stored in the audit trail, and hence not known to any users. It also ensures that valid authentication data is not disclosed to unauthorized individuals;

d.O.E_CONSISTENCY - which ensures that access is granted to individuals on a basis consistent across all platforms. This avoids possible duplication of authentication data.

e.O.E_BOOT – to ensure that information cannot be accessed by booting an alternative operating system

f.O.E_CONNECT- which states that those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets.

g.O.E_PHYSICAL which states that those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security object

[T.MODIFY] *Unauthorized modification or destruction of information by an authorized user of the TOE.*

The security objective O.DISCRETIONARY_ACCESS provides the means to ensure that users can protect the integrity of the information they own or are responsible for.

Security objective O.AUTHORIZATION and O.KNOWN support O.DISCRETIONARY_ACCESS in countering this threat by ensuring that an authorized user cannot impersonate another authorized user, thereby undermining the intent of O.DISCRETIONARY_ACCESS. O.MANAGE ensures that the administrative users can control access to the information.

O.AUDITING helps counter this threat by ensuring that repeated [unsuccessful] attempts to modify information to which the user is not granted permission, can be detected, thereby allowing the administrator to take action before the attack is successful. O.ACCOUNT states that the TOE must ensure that all users can be held accountable for their security relevant actions.

O.ENFORCEMENT supports this threat by ensuring the access control functions are always invoked and cannot be bypassed.

Role based access to the information is covered by the objectives O.DUTY and O.ROLE which ensure that only those users are assigned roles and only those users that have been assigned the correct role can access the information.

Support is also provided by the following security objectives for the environment:

a.O.E_INFO_PROTECT and O.E_PROTECT - ensures that information transmitted over the network is not accessible to other authorized users of the TOE and hence the data cannot be modified or destroyed;

b.O.E_ADMIN ensures that the default access permissions are set appropriately so that access is granted, by default, to a restricted set of users.

c.O.E_BOOT - to ensure that information cannot be accessed by booting an alternative operating system

d.O.E_PHYSICAL which states that those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.

[T.ADMIN_RIGHTS] *Unauthorized use of facilities which require administration rights by an authorized user of the TOE.*

Administration of the TOE has been divided into user roles. The objective for this functionality is divided between O.DUTY, O.HIERARCHICAL and O.ROLE, which ensures that roles are properly defined.

O.DUTY provides the capability of enforcing separation of files and O.HIERARCHICAL allows for the hierarchical definition of these roles. O.ROLE ensures that a user cannot access or perform operations on its resources or objects unless they have been assigned the appropriate role.

O.AUTHORIZATION and O.KNOWN ensures that only authorized users can access the TOE, and provides for identification of users to determine the administration right assigned to the user.

O.AUDITING discourages the unauthorized use of administrator facilities by ensuring that any such breach of security policy can be detected. O.ACCOUNT states that the TOE must ensure that all users can be held accountable for their security relevant actions.

O.MANAGE and O.ENFORCEMENT support this threat by ensuring:

-the database of authorized administrators is properly managed and maintained;

-the administration functions are always checked when invoked and cannot be bypassed;

-the auditing functions are set up appropriately to detect repeated attempts to use the administration functions by non-administrative users.

Support is also provided by the following security objectives for the environment :

O.E_CREDEN ensures user's authentication data is kept secure. This prevents an authorized user impersonating an administrator to gain unauthorized access to administrator facilities.

O.E_CONSISTENCY ensures that a single set of administration rights exist across the TOE, thereby avoiding errors caused by duplication or erroneous entries in the authorization data.

O.E_CONNECT- which states that those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets.

O.E_BOOT - o ensure that information cannot be accessed by booting an alternative operating system

O.E_ACCOUNTABLE ensures that users are uniquely identified and the use of privileged facilities can be controlled amongst the user community.

O.E_SOFTWARE_IN ensures that only administrators can introduce software into the TOE and hence counters the threat of malicious software being introduced. The introduction of some software e.g. Compilers, may provide enhanced facilities to an attacker which could be used to mount a successful attack on the TOE and hence make unauthorized use of administration facilities.

O.E_PHYSICAL which states that those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.

[T.COMPROMISE] *Data may be compromised in terms of confidentiality and integrity if an unauthorized User intercepts a communication link between the TOE and another trusted IT product (which may be another instantiation of the TOE) and attempts to modify information in a way that can not be detected by the TOE or the other trusted IT product.*

This threat is countered by the O.TRUSTPATH objective which states that the TSF must be designed and implemented in a manner that allows for establishing a trusted channel or communication path between the TOE and another trusted IT product that protects the user data transferred over this channel from disclosure and undetected modification.

[T.TRANSIT] *Data transferred between platforms is disclosed or modified to unauthorized users or processes either directly or indirectly (e.g. through spoofing of server/workstation identity).*

Administrators must ensure that data transferred between platforms i.e. along network cabling, is suitably protected against physical or other (e.g. tempest) attacks which may result in the disclose, modification or delay of information transmitted between platforms. Environmental objective O.E_PROTECT ensures this is achieved. Because such issues need to be considered at installation time, environmental objectives O.E_INSTALL and O.E_INFO_PROTECT are also applicable.

[T.OPERATE] *Compromise of IT assets may occur because of improper administration and operation of the TOE.*

This threat is countered by O.ENTRY which states that the TOE must prevent logical entry to it by persons or processes with no rights to access it.

O.MANAGE and O.ENFORCEMENT support this threat by ensuring:

- the database of authorized administrators is properly managed and maintained;
- the administration functions are always checked when invoked and cannot be bypassed;
- the auditing functions are set up appropriately to detect repeated attempts to use the administration functions by non-administrative users.

Support is also provided by the following security objectives for the environment:

O.E_CREDEN ensures user's authentication data is kept secure. This prevents an authorized user impersonating an administrator to gain unauthorized access to administrator facilities.

O.E_CONSISTENCY ensures that a single set of administration rights exist across the TOE, thereby avoiding errors caused by duplication or erroneous entries in the authorization data.

O.E_CONNECT- which states that those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets.

O.E_ACCOUNTABLE ensures that users are uniquely identified and the use of privileged facilities can be controlled amongst the user community.

O.E_ADMIN which states that those responsible for administering the TOE must be competent and trustworthy in order to manage the security functions effectively. Effective management is necessary in order that the threats are not inadvertently or deliberately realized;

O.E_PHYSICAL which states that those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.

[T.ROLEDEV] *The development and assignment of user roles may be done in a manner that undermines security.*

Administration of the TOE has been divided into user roles. The objective for this functionality is divided between O.DUTY, O.HIERARCHICAL and O.ROLE, which ensures that roles are properly defined.

O.DUTY provides the capability of enforcing separation of files and O.HIERARCHICAL allows for the hierarchal definition of these roles. O.ROLE ensures that a user cannot access or perform operations on its resources or objects unless they have been assigned the appropriate role.

O.AUTHORIZATION and O.KNOWN ensures that only authorized users can access the TOE, and provides for identification of users to determine the administration right assigned to the user.

O.AUDITING discourages the unauthorized use of administrator facilities by ensuring that any such breach of security policy can be detected. O.ACCOUNT states that the TOE must ensure that all users can be held accountable for their security relevant actions.

O.MANAGE and O.ENFORCEMENT support this threat by ensuring:

- the database of authorized administrators is properly managed and maintained;
- the administration functions are always checked when invoked and cannot be bypassed;
- the auditing functions are set up appropriately to detect repeated attempts to use the administration functions by non-administrative users.

Support is also provided by the following security objectives for the environment:

O.E_CREDEN ensures user's authentication data is kept secure. This prevents an authorized user impersonating an administrator to gain unauthorized access to administrator facilities.

O.E_CONSISTENCY ensures that a single set of administration rights exist across the TOE, thereby avoiding errors caused by duplication or erroneous entries in the authorization data.

O.E_CONNECT- which states that those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets.

O.E_ACCOUNTABLE ensures that users are uniquely identified and the use of privileged facilities can be controlled amongst the user community

7.2.2 Complete Coverage - Policy

This section provides evidence demonstrating coverage of the Organizational Security Policy by the IT security objectives.

[P.AUTH] Only those users who have been authorized to access the information within the system may access the system.

This policy is implemented through the objective O.AUTHORIZATION which ensures that only authorized users are allowed access to the system. O.MANAGE and O.ENFORCEMENT support this policy by ensuring that the set of authorized users is effectively managed and that the authorization functions are always invoked and cannot be bypassed.

The environmental objective O.E_CREDEN supports this policy by ensuring that authorization data is constructed in a manner commensurate with the protection required for the information on the TOE and that passwords are not disclosed since doing so would compromise the policy.

[P.DAC] The right to access specific data objects is determined on the basis of:

- a.the owner of the object; and
- b.the identity of the subject attempting the access; and
- c.the implicit and explicit access rights to the object granted to the subject by the object owner.

P.DAC is implemented through the objective O.DISCRETIONARY_ACCESS which provides the means of controlling access between objects and subjects on the attributes defined by the policy, and is supported by O.RESIDUAL_INFO objective which ensures that information will not given to users which do not have a need to know, when resources are reused. O.ENFORCEMENT supports this policy by ensuring that the access control functions are always invoked and cannot be bypassed. O.MANAGE supports this policy by requiring authorized administrator be able to manage the functions.

[P.MAC] The system must limit the access to information based on sensitivity, as represented by a label, of the information contained in objects, and the formal clearance of users, as represented by subjects, to access that information. The access rules enforced prevent a subject from accessing information which is of higher sensitivity than it is operating at and prevent a subject from causing information from being downgraded to a lower sensitivity.

The method for classification of information is made based on criteria set forth by the 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 classification of information is outside the scope of the IT system; the IT system is only expected to enforce the classification rules, not determine classification.

The method for determining clearances is also outside the scope of the IT system. It is essentially based on the trust placed in individual users by the organization.

P.MAC is implemented through the objective O.MANDATORY_ACCESS which provides the means of controlling access between subjects and objects on the attributes (i.e., sensitivity labels) by the policy, and is supported by O.RESIDUAL_INFO objective which ensures that information will not given to users which do not have a need to know, when resources are reused. O.ENFORCEMENT supports this policy by ensuring that the access control functions are always invoked and cannot be bypassed. O.MANAGE supports this policy by requiring authorized administrator be able to manage the functions.

[P.ACCOUNTABLE] The users of the system shall be held accountable for their actions within the system.

Accountability is implemented primarily through the objective O.AUDITING which ensures user's security relevant events can be recorded so as to be able to hold users accountable for their actions. O.ACCOUNT ensures that all users can be held accountable for their security relevant actions. An unauthorized user can not be held accountable for their actions and O.AUTHORIZATION therefore supports this policy by ensuring that only authorized users are allowed access. O.MANAGE and O.ENFORCEMENT support this policy by ensuring that an effective set of actions are audited in order to detect attempted breaches of the security policy and that the auditing functions are always invoked and cannot be bypassed.

Environmental objectives O.E_ADMIN, O.E_ACCOUNTABLE and O.E_AUDITDATA ensure that the administrator manages the auditing security functions effectively.

[P.NEED_TO_KNOW] The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a “need to know” for that information.

P.NEED_TO_KNOW is implemented primarily through the objective O.DISCRETIONARY_ACCESS which provides the means of controlling access between objects and subjects on the attributes defined by the policy, and is supported by O.RESIDUAL_INFO objective which ensures that information will not given to users which do not have a need to know, when resources are reused. O.ENFORCEMENT supports this policy by ensuring that the access control functions are always invoked and cannot be bypassed. O.MANAGE supports this policy by requiring authorized administrator be able to manage the functions. O.TRUSTPATH supports this policy by requiring that the TSF be designed and implemented in a manner that allows for establishing a trusted channel or communication path between the TOE and another trusted IT product.

7.2.3 Complete Coverage - Environmental Assumptions

This section provides evidence demonstrating coverage of the environmental assumptions by security objectives.

[A.PROTECT] *It is assumed that all network and peripheral cabling is approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted.*

The environmental objective O.E_PROTECT ensures that network cabling is suitably protected against threats of modification, tampering or interruption of the data transmitted via this medium. O.E_INFO_PROTECT ensures that, where the cabling is carrying classified information, that the infrastructure has been approved. O.E_CONNECT ensures that no connections to outside systems or users undermine the security of IT assets.

[A.LOCATE] *It is assumed that the processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.*

The environmental objective O.E_PHYSICAL states that those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.

[A.ASSET] *It is assumed that the value of the stored assets merits moderately intensive penetration or masquerading attacks.*

The environmental objective O.E_PROTECT ensures that network cabling is suitably protected against threats of modification, tampering or interruption of the data transmitted via this medium. O.E_INFO_PROTECT ensures that, where the cabling is carrying classified information, that the infrastructure has been approved. O.E_CONNECT ensures that no connections to outside systems or users undermine the security of IT assets.

7.2.4 Complete Coverage - Personnel Assumptions

[A.ACCESS] *It is assumed that 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 TOE administrator. These roles adequately reflect the users job function, responsibilities, qualifications, and/or competencies within the enterprise.*

The environmental objective O.E_ACCOUNTABLE ensures that only approved groups of users for which the product was accredited may access the system and that each user is assigned a unique user ID.

[A.MANAGE] *There will be one or more competent and trustworthy individuals assigned to manage TOE security. These individuals will have sole responsibility for the following functions:*

- a. create and maintain roles;
- b. establish and maintain relationships among roles
- c. Assignment and revocation of users to roles

In addition, these individuals, as owners of the entire corporate data, along with object owners, will have the ability to assign and revoke object access rights to roles.

The assumption A.MANAGE is covered by all environmental objectives, specifically O.E_ADMIN, O.E_ACCOUNTABLE, O.E_AUDITDATA, O.E_CREDEN, O.E_BOOT, O.E_CONNECT, O.E_CONSISTENCY, O.E_INSTALL, O.E_INFO_PROTECT, O.E_MAINTENANCE, O.E_RECOVER, O.E_PHYSICAL, O.E_SOFTWARE_IN, O.E_SERIAL_LOGIN and O.E_PROTECT. All of these objectives require that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

[A.OWNER] *Assumes a limited set of users is given the rights to “create new data objects” and they become owners for those data objects. The organization is the owner of the rest of information under the control of the TOE.*

[A.NO_EVIL_ADM] *Assumes that system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.*

This assumption is covered by the environmental objective O.E_ADMIN which states that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains. It is also covered by O.E_INSTALL which requires procedures for secure distribution, installation and configuration of systems.

[A.COOP] *Assumes that 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.*

This assumption is met by the environmental objective O.E_CREDEN which requires the safe storage of authentication data and ensures that users will not disclose their passwords

7.2.5 Complete Coverage - Procedural Assumptions

[A.USER] *Each individual user must have a unique user ID.*

This is primarily met by O.E_ACCOUNTABLE which states that each individual user is assigned a unique user ID. This is supported by O.E_ADMIN and O.E_CREDEN which ensure that those responsible for the TOE are competent and that the user IDs are not disclosed to unauthorized individuals.

[A.PASSWORD] *It is assumed that the length of password for normal users will be at least 8 characters.*

This is primarily met by O.E_INSTALL which states that 'Those responsible for the TOE must establish and implement procedures to ensure that the software components are configured in a secure manner'. It is also supported by O.E_ADMIN which ensures that the administrator is competent enough to ensure this setting within the TOE remains set.

[A.CLEARANCE] *Procedures exist for granting users authorization for access to specific security levels.*

This is primarily met by O.E_CREDEN which requires procedures to ensure that users are assigned appropriate clearances.

[A.SENSITIVITY] *Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all output generated.*

This is primarily met by O.E_CREDEN which requires procedures to ensure that objects are assigned appropriate sensitivity labels.

[A.LDAP_DOMAINS] *It is assumed that, if the product comprises more than one platform, all platforms are administered from a central point within each LDAP domain.*

LDAP is installed and configured at installation time, and therefore objective O.E_CONSISTENCY ensures this assumption is upheld.

[A.BRIDGES&ROUTERS] *All bridges and routers are assumed to correctly pass data without modification.*

As for A.Protect, this assumption is met by O.E_PROTECT and O.E_INFO_PROTECT; bridges and routers are part of the cabling infrastructure.

[A.CONNECT] *It is assumed that all connections to peripheral devices reside within controlled access facilities. Internal communication paths to interface points such as terminals are assumed to be adequately protected.*

This assumption is met by the following environmental objectives:

O.E_SERIAL_LOGIN which ensures the protection of attached serial login devices.

O.E_PROTECT which ensures that data transferred between servers and workstations is protected

O.E_PHYSICAL which ensures that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.

[O.E_CONSISTENCY] which ensures that data is set up and maintained in a consistent manner across all platforms in the distributed system.

[A.PEER] It is assumed that 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.

The assumption A.PEER is met by the environmental objective O.E_INSTALL which states that those responsible for the TOE must ensure that the TOE hardware, software and firmware components that comprise the networked product are distributed, installed and configured in a secure manner.

7.3 Security Requirements Rationale

This section demonstrates that the set of security requirements is suitable to meet and is traceable to the set of security objectives.

7.3.1 Complete Coverage - Objectives

This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

Table 7-5 Security Objectives to Functional Component Mapping

Objective	SFR
O.AUTHORIZATION	User Attribute Definition (FIA_ATD.1)
	Strength of Authentication Data (FIA_SOS.1)
	Authentication (FIA_UAU.1)
	User Authentication Before Any Action (FIA_UAU.2)
	Protected Authentication Feedback (FIA_UAU.7)
	User Identification Before Any Action (FIA_UID.2)
	User Identification (FIA_UID.1)
	TSF Initiated Screen Locking (FTA_SSL.1)
	User initiated locking (FTA_SSL.2)
	Trusted Path (FTP_TRP.1)
O.ENTRY	Management of User Attributes (FMT_MTD.1)
	Management of Authentication Data (FMT_MTD.1)
	Revocation of User and/or Object Attributes (FMT_REV.1)
	Security Management Roles (FMT_SMR.1)

Table 7-5 Security Objectives to Functional Component Mapping

Objective	SFR
O.DISCRETIONARY_ACCESS	Discretionary Access Control Policy (FDP_ACC.1)
	Discretionary Access Control Functions (FDP_ACF.1)
	User Attribute Definition (FIA_ATD.1)
	User-subject Binding (FIA_USB.1)
	Management of Object Security Attributes (FMT_MSA.1)
	Secure Security Attributes (FMT_MSA.2)
	Static Attribute Initialization (FMT_MSA.3)
	Revocation of Object Attributes (FMT_REV.1)
O.MANDATORY_ACCESS	Export of Unlabeled User Data (FDP_ETC.1)
	Export of Labeled User Data (FDP_ETC.2)
	Mandatory Access Control Policy (FDP_IFC.1)
	Mandatory Access Control Functions (FDP_IFF.2)
	Import of Unlabeled User Data (FDP_ITC.1)
	Import of Labeled User Data (FDP_ITC.2)
	User Attribute Definition (FIA_ATD.1)
	User-subject Binding (FIA_USB.1)
	Management of Object Security Attributes (FMT_MSA.1)
	Secure Security Attributes (FMT_MSA.2)
	Static Attribute Initialization (FMT_MSA.3)
	Revocation of Object Attributes (FMT_REV.1)
O.KNOWN	Authentication (FIA_UAU.1)
	User Authentication Before Any Action (FIA_UAU.2)
	User Identification (FIA_UID.1)

Table 7-5 Security Objectives to Functional Component Mapping

Objective	SFR
O.AUDITING	Audit Data Generation (FAU_GEN.1)
	User Identity Generation (FAU_GEN.2)
	Audit Review (FAU_SAR.1)
	Restricted Audit Review (FAU_SAR.2)
	Selectable Audit Review (FAU_SAR.3)
	Selective Audit (FAU_SEL.1)
	Guarantees of Audit Data Availability (FAU_STG.1)
	Action in case of Possible Audit Loss (FAU_STG.3)
	Prevention of Audit Data Loss (FAU_STG.4)
	User Subject Binding (FIA_USB.1)
	Management of the Audit Trail (FMT_MTD.1)
	Management of the Audited Events (FMT_MTD.1)
	Reliable Time Stamps (FPT_STM.1)
O.ACCOUNT	Audit Data Generation (FAU_GEN.1)
	User Identity Generation (FAU_GEN.2)
	User Subject Binding (FIA_USB.1)
	Restricted Audit Review (FAU_SAR.2)
	Selectable Audit Review (FAU_SAR.3)
	Selective Audit (FAU_SEL.1)
	Guarantees of Audit Data Availability (FAU_STG.1)
	Prevention of Audit Data Loss (FAU_STG.4)
	Reliable Time Stamps (FPT_STM.1)
	Audit Review (FAU_SAR.1)
	Management of User Attributes (FMT_MTD.1)
O.TRUSTPATH	Inter-TSF Trusted Channel (FTP_ITC.1)
	Trusted Path (FTP_TRP.1)
	Basic data exchange confidentiality (FDP_UCT.1)
	Data Exchange Integrity (FDP_UIT.1)
O.RESIDUAL_INFO	Subject Residual Information Protection (FDP_RIP.2)

Table 7-5 Security Objectives to Functional Component Mapping

Objective	SFR
O.MANAGE	Audit Review (FAU_SAR.1)
	Restricted Audit Review (FAU_SAR.2)
	Selectable Audit review (FAU_SAR.3)
	Selectable Audit (FAU_SEL.1)
	Action in case of Possible Audit Data Loss (FAU_STG.3)
	Prevention of Audit Data loss (FAU_STG.4)
	Management of Audit Trail (FMT_MTD.1)
	Management of Audit Events (FMT_MTD.1)
	Management of User Attributes (FMT_MTD.1)
	Management of Authentication Data (FMT_MTD.1)
	Revocation of User Attributes (FMT_REV.1)
	Security Management Roles (FMT_SMR.1)
	Specification of Management Functions (FMT_SMF.1)
	Management of Security Attributes (FMT_MSA.1)
	Secure Security Attributes (FMT_MSA.2)
	Static Attribute Initialization (FMT_MSA.3)
	Secure TSF Data (FMT_MTD.3)
	O.ENFORCEMENT
Reference Mediation (FPT_RVM.1)	
Domain Separation (FPT_SEP.1)	
TSF Self test (FPT_TST.1)	
Trusted Path (FTP_TRP.1)	
O.DUTY	Security Roles (FMT_SMR.2)
O.HIERACHICAL	Security Roles (FMT_SMR.2)

Table 7-5 Security Objectives to Functional Component Mapping

Objective	SFR
O.ROLE	RBAC Policy (FDP_ACC.1)
	RBAC Functions (FDP_ACF.1)
	Management of Object Security Attributes (FMT_MSA.1)
	Static Attribute Initialization (FMT_MSA.3)
	Management of User Attributes (FMT_MTD.1)
	Security Roles (FMT_SMR.2)
	Limitation on the Scope of Selectable Attributes (FTA_LSA.1)
	TOE Session Establishment (FTA_TSE.1)

O.AUTHORIZATION

The TSF must ensure that only authorized users gain access to the TOE and its resources.

Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UID.2 and FIA_UAU.2]. To ensure authorized access to the TOE, authentication data is protected [FIA_ATD.1, FIA_UAU.7, FMT_MTD.1 and FTP_TRP.1]. The strength of the authentication mechanism must be sufficient to ensure unauthorized users cannot pose as authorized users with reasonable time, effort and other constraints [FIA_SOS.1]. Lock screen can be initiated to ensure that only authorized users can gain access [FTA_SSL.1 and FTA_SSL.2].

O.ENTRY

The TOE must prevent logical entry to it by persons or processes with no rights to access it.

The TSF shall restrict the ability to create, modify and initialize the user security attributes, other than authentication data, to authorized administrators (FMT_MTD.1). The TSF shall restrict the ability to create, modify and initialize the authentication data to authorized administrators or users authorized to modify their own authentication data (FMT_MTD.1). The TSF shall restrict the ability to revoke user or object attributes within the TSC to authorized administrators (FMT_REV.1). The TSF shall maintain all roles and be able to associate users with roles (FMT_SMR.1).

O.DISCRETIONARY_ACCESS

The TSF must provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the P.DAC security policy.

Discretionary access control must have a defined scope of control [FDP_ACC.1]. The rules of the DAC policy must be defined [FDP_ACF.1]. The security attributes of objects used to enforce the DAC policy must be defined [FDP_ACF.1]. The security attributes of subjects used to enforce the DAC policy must be defined [FIA_ATD.1 and FIA_USB.1]. Authorized users must be able to control who has access to objects [FMT_MSA.1], that only secure values are set for security attributes [FMT_MSA.2] and be able to revoke that access [FMT_REV.1]. Protection of named objects must be continuous, starting from object creation [FMT_MSA.3].

O.MANDATORY_ACCESS

The TSF must limit the access of objects by subjects based on sensitivity labels outside the control of normal users and in accordance with the set of rules defined by the P.MAC security policy.

Mandatory access control must have a defined scope of control [FDP_IFC.1]. The rules of the MAC policy must be defined [FDP_IFF.2]. The security attributes of objects used to enforce the MAC policy must be defined [FDP_IFF.1]. The security attributes of subjects used to enforce the MAC policy must be defined [FIA_ATD.1 and FIA_USB.1]. Authorized users must be able to control applicable security attributes [FMT_MSA.1], that only secure values are set for security attributes [FMT_MSA.2] and be able to revoke that access [FMT_REV.1]. Protection of objects must be continuous, starting from object creation [FMT_MSA.3]. Furthermore, there must be well defined rules for importing labeled [FDP_ITC.2] and unlabeled [FDP_ITC.1] data and exporting labeled [FDP_ETC.2] and unlabeled [FDP_ETC.1] data.

O.KNOWN

Legitimate users of the system must be identified before rights of access can be granted.

The TSF shall allow TSF mediated actions on behalf of the user to be performed before the user is authenticated (FIA_UAU.1). The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of the user (FIA_UAU.1). The TSF shall allow TSF mediated actions on behalf of the user to be performed before the user is identified (FIA_UID.1). The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on the behalf of the user (FIA_UID.1 and FIA_UAU.2).

O.AUDITING

The TOE must provide the means of recording any security relevant events, so as to (a) assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack; and (b) hold users accountable for any actions they perform that are relevant to security.

Security-relevant actions must be defined, auditable [FAU_GEN.1], and capable of being associated with individual users [FAU_GEN.2 and FIA_USB.1]. The audit trail must be protected so that only authorized users may access it [FAU_SAR.2]. The TSF must provide the capability to audit the actions of an individual user [FAU_SAR.3, FAU_SEL.1 and FIA_USB.1]. The audit trail must be complete [FAU_STG.1 and FAU_STG.4]. The time stamp associated must be reliable [FPT_STM.1]. An authorized administrator must be able to review [FAU_SAR.1] and manage [FAU_STG.3.1 and FMT_MTD.1] the audit trail.

O.ACCOUNT

The TOE must ensure that all users can be held accountable for their security relevant actions.

Security-relevant actions must be defined, auditable [FAU_GEN.1], and capable of being associated with individual users [FAU_GEN.2 and FIA_USB.1]. The audit trail must be protected so that only authorized users may access it [FAU_SAR.2]. The TSF must provide the capability to audit the actions of an individual user [FAU_SAR.3, FAU_SEL.1 and FIA_USB.1]. The audit trail must be complete [FAU_STG.1 and FAU_STG.4]. The time stamp associated must be reliable [FPT_STM.1]. An authorized administrator must be able to review [FAU_SAR.1] and manage [FAU_SAR.3.1 and FMT_MTD.1] the audit trail.

O.TRUSTPATH

The TSF must be designed and implemented in a manner that allows for establishing a trusted channel or communication path between the TOE and another trusted IT product that protects the user data transferred over this channel from disclosure and undetected modification.

The TSF must be able to establish (a) an Inter-TSF trusted channel between itself and another trusted IT product and/r (b) a communication path between itself and remote or local users or that is logically distinct from other communication paths [FTP_ITC.1] [FTP_TRP.1] protecting the user data transferred from disclosure [FDP_UCT.1] and undetected modification [FDP_UIT.1].

O.RESIDUAL_INFO

The TSF must ensure that any information contained in a protected resource is not released when the resource is recycled.

Residual information associated with defined objects in the TOE must be purged prior to the reuse of the object containing the residual information [FDP_RIP.2].

O.MANAGE

The TSF must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

Aspects that need to be managed must be defined [FMT_SMF.1]. The TSF must provide for an authorized administrator to manage the TOE [FMT_SMR.1]. The administrator must be able to administer user accounts [FMT_MTD.1 and FMT_REV.1]. The administrator must be able to review and manage the audit trail [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.3, FAU_STG.4, FMT_MTD.1]. Only secure values must be accepted for RBAC-related attributes and TSF data [FMT_MSA.2, FMT_MTD.3]. The administrator must be able to ensure that only authorized users are able to control who has access to objects [FMT_MSA.1], and that only secure values are set for security attributes [FMT_MSA.2].

The TSF shall provide a secure state following failure and allow manual and function recovery [FPT_FLS.1, FPT_RCV.1, FPT_RCV.4].

O.ENFORCEMENT

The TOE security policy is enforced in a manner which ensures that the organizational policies are enforced in the target environment i.e. the integrity of the TSF is protected. The TSF must make and enforce the decisions of the TSP [FPT_RVM.1]. It must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]. Additionally, the TOE must provide the capability to demonstrate correct operation of the TSF's underlying abstract machine [FMT_AMT.1]. The correctness of this objective is further met through the assurance requirements defined in the PP.

The TSF shall run a suite of self tests to demonstrate the correct operation of the TOE [FPT_TST.1]. The integrity of the TOE is enforced via the trusted path [FTP_TRP.1]

O.DUTY

The TOE must provide the capability of enforcing separation of duties, so that no single user is required to perform all administrative functions.

The TSF shall be able to associate users with roles [FMT_SMR.2].

O.HIERARCHICAL

The TOE must allow hierarchical definitions of roles. Hierarchical definition of roles means that they are constructed hierarchically using rights profiles.

The TSF shall ensure that the set of administrative roles can modify security attributes for all objects under the control of the TOE [FMT_SMR.2].

O.ROLE

The TOE must prevent users from gaining access to and performing operations on its resources and objects unless they have been granted access by the resource or objects owner or have been assigned a role which permits those operations.

The TSF shall enforce an RBAC policy [FDP_ACC.1 and FDP_ACF.1]. User and object security attributes required to enforce the RBAC policy must be securely managed [FMT_MTD.1, FMT_MSA.1 and FMT_MSA.3]. The TSF shall be able to associate users with roles [FMT_SMR.2]. The TSF shall deny and restrict the scope of a session [FTA_LSA.1 and FTA_TSE.1].

Table 7-6 Dependencies between Functional Components

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFE.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SME.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1	
FAU_GEN.1																		x					
FAU_GEN.2	x									x													
FAU_SAR.1	x																						
FAU_SAR.2		x																					
FAU_SAR.3		x																					
FAU_SEL.1	x													x									

Table 7-6 Dependencies between Functional Components

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_ITE.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FPT_ITC.1	FPT_TRP.1	
FAU_STG.1	x																						
FAU_STG.3			x																				
FAU_STG.4			x																				
FDP_ACC.1					x						x												
FDP_ACF.1				x								x											
FDP_ETC.1						x																	
FDP_ETC.2						x																	
FDP_IFC.1							x																
FDP_ITE.1						x						x											
FDP_ITC.1						x						x											
FDP_ITC.2						x													X			x	
FDP_RIP.2																							
FIA_ATD.1																							
FIA_SOS.1																							
FIA_UAU.2										x													
FIA_UAU.7									x														
FIA_UID.2																							
FIA_USB.1							x																
FMT_MSA.1				x							x	x			x	x							
FMT_MSA.2				x							x					x							
FMT_MSA.3					x						x					x							
FMT_MTD.1															x	x							
FMT_MTD.3														x									
FMT_REV.1																x							
FMT_SMF.1																							
FMT_SMR.1									x			x											
FMT_SMR.2									⊕														
FPT_AMT.1																							
FPT_FLS.1																							

Table 7-6 Dependencies between Functional Components

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1	
FPT_RCV.1																							
FPT_RCV.4																							
FPT_RVM.1																							
FPT_SEP.1																							
FPT_STM.1																							
FPT_TST.1																	☑						
FTA_LSA.1																							
FTA_SSL.1									☑														
FTA_SSL.2									☑														
FTA_TSE.1																							
FDP_UCT.1				☑																		☑	☑
FDP_UIT.1				☑																		☑	☑
FMT_SMF.1																							
FTP_ITC.1																							
FTP_TRP.1																							

7.3.2 Requirements are Mutually Supportive and Internally Consistent

The above table, Table 7-6, identifies the dependencies of all functional components included in the ST. Required dependencies are indicated by the use of the checkmark: ☑. All dependencies between functional components are satisfied within this ST, with the following exceptions.

- Dependencies on FIA_UAU.1 and FIA_UID.1 are satisfied, respectively, by the inclusion of FIA_UAU.2 and FIA_UID.2 which are hierarchic to these components.
- The dependency on FDP_IFC.1 are satisfied by FDP_IFF.2 rather than FDP_IFF.1 which is hierarchic to the component.
- The CC indicates that FDP_ITC.2 is dependent on FPT_TDC.1. First, it should be noted that the [LSPP] introduces FDP_ITC.2 without including FPT_TDC.1 and offers no explanation. FDP_ITC.2 requires that certain rules are applied when importing labeled data while FPT_TDC.1 requires consistent interpretation of specified data between products. While this may seem a necessary relationship, FDP_ITC.2 includes elements that dictate that the security attributes must be unambiguously associated with the data and the interpretation of security attributes

must be as intended by the source. Hence, it seems as though FPT_TDC.1 is redundant and is therefore not necessary. Given this and the fact that it was excluded in the [LSPP] it was excluded also from this ST.

ALC_FLR.3 introduces no additional dependencies.

7.3.3 Justification for Choice of Assurance Requirements

This ST claims an assurance rating of EAL4+. The ST has been based largely on [CAPP], [LSPP], and [RBAC] which specific security requirements for a product which is to be used in a non-hostile environment with a moderate risk to the assets. In such environments, an assurance level of EAL3 is recommended as stated in [CAPP] and [LSPP].

This ST also contains the assurance requirements from the CC EAL4 assurance package augmented with ALC_FLR.3. The CC allows assurance packages to be augmented, which allows the addition of assurance components from the CC not already included in the EAL. Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures and correcting security flaws. This ST is based on solid rigorous commercial software development practices and has been developed for a generalized environment for a TOE that is generally available and does not need modification to meet the security needs specified in the ST.

The EAL chosen is based on the statement of the security environment and objectives defined in this ST. The sufficiency of the EAL chosen is justified based on the enhancements made to [CAPP], [LSPP], and [RBAC] which are detailed in Section 5.1. and the flaw remediation procedures defined in supplement ALC_FLR.3.

[CAPP] and [LSPP] require an EAL3 assurance rating. EAL4+ is a super-set of those requirements.

[RBAC] requires EAL2 assurance augmented with ADV_SPM.1.1 EAL4+ is a super-set of these requirements.

7.3.4 Strength of Function Claim is Consistent with Security Objectives

The claimed strength of function rating is SOF-medium. This exceeds the [RBAC] requirement of SOF-basic and is consistent with [CAPP] and [LSPP] which states that a 'one off' probability of guessing the password shall be 1,000,000. This is specified in SFR FIA_SOS.1 which is in turn consistent with the security objectives described in section 7.3.

7.4 TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

7.4.1 IT Security Functions Satisfy Functional Requirements

This section demonstrates that the combination of the specified TOE IT security functions work together so as to satisfy the TOE security functional requirements. The table below shows the TOE security functions which together satisfy each security functional requirement. They are grouped under the relevant TOE security objective.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Audit Data Generation (FAU_GEN.1.1)	Audit.1 to Audit.11, Audit.15 ^a Auditing procedures provide a record of auditable events.
Audit Data Generation (FAU_GEN.1.2)	Audit.1,2,3,4,5,6,8,11,21 Event records include date and time of the event, subject identity and the outcome (success or failure) of the event.
User Identity Generation (FAU_GEN.2.1)	Audit.1 to Audit.11 Auditing procedures identify each auditable event with the identity of the user that caused the event.
Audit Review (FAU_SAR.1.1)	Audit.19 Authorized administrators of the TOE have the capability to read all audit record information.
Audit Review (FAU_SAR.1.2)	Audit.19 Audit records are suitable for user interpretation.
Restricted Audit Review (FAU_SAR.2.1)	Audit.14 Audit data is protected so that access is limited to administrative users.
Selectable Audit Review (FAU_SAR.3.1)	Audit.19 Administrative users are able to selectively retrieve audit data based on, at a minimum, the identity of users, the type of audit event, and the audit class.
Selective Audit (FAU_SEL.1.1)	Audit.17, Audit.18 Administrative users are able to define the default system audit-mask that defines which audit classes are recorded by default. Only administrative users are able to define a per-user audit-mask that defines which audit classes are recorded for that user. For a given user, the system shall audit those classes that are in the default system audit mask or the per-user audit mask.
Protected Audit Trail Storage (FAU_STG.1.1)	Audit.14 Audit data is protected against unauthorized deletion because access to it is limited to administrative users.
Protected Audit Trail Storage (FAU_STG.1.2)	Audit.14 Audit data is protected against modification.
Action in Case of Possible Audit Data Loss (FAU_STG.3.1)	Audit.23 The system shall notify an administrator of audit trail saturation.
Prevention of Audit Data Loss (FAU_STG.4.1)	Audit.20, Audit.21 In the event of an audit storage failure the system will prevent auditable events, except those taken by the administrator.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Discretionary Access Control Policy (FDP_ACC.1.1)	DAC.6, Admin.2, Admin.3 The access permissions on an owner controlled object can be modified only by a subject that owns the object or by a user with override file access permissions.
Discretionary Access Control Functions (FDP_ACF.1.1)	DAC.3, DAC.4 Trusted Extensions file permissions ensure that no subject can change the owner or group of an owner controlled object unless it has override file access permissions, or optionally is the owner of the object
Discretionary Access Control Functions (FDP_ACF.1.2)	DAC.6 Trusted Extensions file permissions ensure that whenever a subject requests access to an owner controlled object, the access permissions for that object shall be checked to determine whether the user who owns the subject can access the object in the requested mode.
Discretionary Access Control Functions (FDP_ACF.1.3)	DAC.8, Admin.2, Admin.3 Trusted Extensions file permissions ensure that a subject cannot override discretionary access control unless they have override file access permissions
Discretionary Access Control Functions (FDP_ACF.1.4)	DAC.3, DAC.4, DAC.6. Whenever a subject requests access to an owner controlled object, the access permissions for that object will be checked to determine whether the user who owns the subject can access the object in the requested mode. Where an ACL is defined for an object, it will be used instead of the object's permission bits. Unix file permissions ensure that the changes to the object are allowable unless overridden by ACL.
Export of Unlabeled User Data (FDP_ETC.1)	MAC.2, MAC.5, MAC.6, MAC.8 Single-level devices can be defined by an administrator. Any data exported via a single-level device must conform with the MAC policy for writing data and the data will be exported without any label information. Devices are either single- or multi-level and cannot be both.
Export of Labeled User Data (FDP_ETC.2)	MAC.2, MAC.5, MAC.6, MAC.7, MAC.8 Multi-level devices can be defined by an administrator. Any data exported via a multi-level device must conform with the MAC policy for writing data within the defined range of the device. Exported data will be labeled in a manner consistent with the device so the label is unambiguous. Printed output will be appropriately marked at the beginning, end, and each intermediate page. Devices are either single- or multi-level and cannot be both.
Mandatory Access Control Policy (FDP_IFC.1)	MAC.1 All operations between subjects and objects is controlled by the MAC policy.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Mandatory Access Control Functions (FDP_IFF.2)	MAC.1, MAC.3, MAC.4, MAC.5 The MAC policy is implemented using sensitivity labels on subject and objects that serve to allow access decisions to be made based on those attributes using well defined rules.
Import of Unlabeled User Data (FDP_ITC.1)	MAC.2, MAC.5, MAC.6, MAC.8 Single-level devices can be defined by an administrator. Any data imported via a single-level device must conform with the MAC policy for reading data and the data will be imported without any label information. However, labels will be assigned based on the label of the device from which the data is imported. Devices are either single- or multi-level and cannot be both.
Import of Labeled User Data (FDP_ITC.2)	MAC.2, MAC.5, MAC.6, MAC.7, MAC.8 Multi-level devices can be defined by an administrator. Any data imported via a multi-level device must conform with the MAC policy for reading data within the defined range of the device. Imported data will be labeled based on labels received with the data when imported depending on the type of device. Devices are either single- or multi-level and cannot be both.
Object Residual Information Protection (FDP_RIP.2.1)	OR.1, OR.2, OR.3 Trusted Extensions ensures that any previous content of a resource is made unavailable upon the allocation of the resource to all objects.
Subject Residual Information Protection	OR.1, OR.2, OR.3 Trusted Extensions ensures that any previous content of a resource is made unavailable upon the allocation of the resource to all subjects.
Basic Data Exchange Confidentiality (FDP_UCT.1)	DAC.9 The TSF shall enforce the Discretionary Access Control Policy to be able to transmit objects in a manner protected from unauthorized disclosure
Data Exchange Integrity (FDP_UIT.1.1)	DAC.10 The TSF shall enforce the Discretionary Access Control Policy to be able to transmit and receive user data in a manner protected from modification and insertion errors
Data Exchange Integrity (FDP_UIT.1.2)	DAC.10 The TSF shall enforce the Discretionary Access Control Policy to be able to transmit and receive user data in a manner protected from modification and insertion errors
User Attribute Definition (FIA_ATD.1.1)	IA.1, IA.11 Trusted Extensions assures that users are assigned unique individual security attributes that are enforced throughout each session.
Strength of Authentication Data (FIA_SOS.1.1)	IA.1, IA.5, IA.6, IA.8, IA.11 ^b Trusted Extensions mechanisms exists which enforces standards of password management.
Authentication (FIA_UAU.1.1)	IA.1 User must authenticate identity at the beginning of each user session.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Authentication (FIA_UAU.1.2)	IA.1 No user actions are allowed until authentication has completed successfully.
User Authentication (FIA_UAU.2)	IA.1, IA.3, IA.4 No user actions are allowed until authentication has completed successful. Also, accounts are locked after an administrator controlled number of failed authentication attempts and the accounts can be unlocked only be an administrator. This helps ensure that authenticated users are truly authentic.
Protected Authentication Feedback (FIA_UAU.7.1)	IA.9 Passwords are not displayed upon entry.
Identification (FIA_UID.1.1)	IA.1 Trusted Extensions makes an allowance for actions to be taken on behalf of the user prior to identification.
Identification (FIA_UID.1.2)	IA.1 Trusted Extensions requires each user be successfully identified before allowing any other actions on the behalf of that user.
Identification (FIA_UID.2)	IA.1 Trusted Extensions requires each user be successfully identified before allowing any other actions on the behalf of that user.
User-Subject Binding (FIA_USB.1.1)	IA.2 Audit ID data assigned to a user upon entry does not change as the user switches user ID's and roles.
Management of Object Security Attributes (FMT_MSA.1.1)	DAC.1, DAC.2 Discretionary Access Control rules ensure restricted ability to modify the access control attributes associated with a named object. MAC.4 Subject sensitivity labels are constrained by their defined clearance ranges.
Static Attribute Initialization (FMT_MSA.3.1)	DAC.7 When a subject creates a filesystem object, the user ID of the subject is assigned to the object, and the user's umask restricts the initial access permissions of the object. MAC.3 The MAC rules serve to ensure that objects are protected appropriately by the MAC rules by default since every read and write is carefully constrained according to sensitivity labels.
Static Attribute Initialization (FMT_MSA.3.2)	DAC.7 The TOE default is that a user's umask is set to prevent any user other than the owner having write access to the object. MAC.5 Object sensitivity labels can only be changed by a limited set of users.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Management of the Audit Trail (FMT_MTD.1.1)	Audit.14 Access to audit trail is limited to the administrator and therefore protected from unauthorized observation or modification.
Management of Audited Events (FMT_MTD.1.1)	Audit.16, 17, 18 Only the administrative user may initialize or change auditable events.
Management of User Attributes (FMT_MTD.1.1)	IA.11, Admin.1 Only the administrator can initialize user accounts and assign user profiles
Management of Authentication Data (FMT_MTD.1.1)	IA.10 Only the administrator can change user authentication data.
Management of Authentication Data (FMT_MTD.1.1)	IA.11 A user may change their own password.
Management of Authentication Data (FMT_MTD.3)	ENF.4 The TSF ensures that only secure values are accepted for user passwords
Specification of Management Functions (FMT_SMF.1.1)	IA.1, IA.11, DAC.1, DAC.8 TSF allows for the administrator to manage the system security attributes
Revocation of User Attributes (FMT_REV.1.1)	IA.11, DAC.1, DAC.2, Admin.1 Only the administrator can remove or delete user accounts
Revocation of Object Attributes (FMT_REV.1.2)	IA.11 Once a user has been removed from the system there is no way to authenticate.
Revocation of Object Attributes (FMT_REV.1.2)	DAC.6 Trusted Extensions file permissions ensure that only authorized users are able to revoke object attributes. MAC.5 Only a limited set of users can modify sensitivity labels.
Security Management Roles (FMT_SMR.1.1)	DAC.1, DAC.2, IA.11, Admin.1 Trusted Extensions assigns a unique id to each user which enables the assignment of management roles. Only the administrator can assign roles to a user.
Security Management Roles (FMT_SMR.1.2)	DAC.2, DAC.8, IA.11, Audit.14, 16, 17, 18, 19, 22, 23, Admin.1 Trusted Extensions supports this requirement through the use of uid assignment and audit tracking
Restriction on Security Roles (FMT_SMR.2.1)	Admin.1, Admin.4, Admin.5 The TSF shall maintain the list of roles.
Restriction on Security Roles (FMT_SMR.2.2)	Admin.1, Admin.4, Admin.5 The TSF shall be able to associate users with roles.
Restriction on Security Roles (FMT_SMR.2.3)	Admin.4, Admin.5 Defined ability of users and administrators to modify security attributes and objects.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Abstract Machine Testing (FPT_AMT.1.1)	ENF.3 SUN provides a suite of Abstract machine tests for TOE users
Failure with Preservation of Secure State (FPT_FLS.1)	Fail.2 The TSF maintains the ability to preserve RBAC database information when the system experiences a failure
Manual Recovery (FPT_RCV.1)	Fail.1 The TSF will enter maintenance mode following a system failure, allowing the administrator to bring the system to a secure state before resuming operation.
Functional Recovery (FPT_RCV.4)	Fail.2 The TSF maintains the ability to preserve RBAC database information when the system experiences a failure
Reference Mediation (FPT_RVM.1.1)	ENF.1 Trusted Extensions validates all actions between subjects and objects before allowing the action to succeed
Domain Separation (FPT_SEP.1.1)	ENF.2 Trusted Extensions maintains a secure domain within the system kernel for trusted execution and the storage of trusted objects. This are is separate from untrusted activities within the TOE.
Domain Separation (FPT_SEP.1.2)	ENF.2 Trusted Extensions maintains a secure domain within the system kernel for trusted execution and the storage of trusted objects. This are is separate from untrusted activities within the TOE
Reliable Time Stamps (FPT_STM.1.1)	Audit.12 Trusted Extensions provides a reliable time stamp through it's audit mechanism.
TSF Self Test (FPT_TST.1)	ENF.3 The TOE shall allow an administrator to perform a self test to ensure that the underlying TSF is enforcing process separation
TSF-Limitation on scope of selectable attributes (FTA_LSA.1.1)	Admin.5 The TSF shall restrict the scope of a session based on the role assigned to the user.
TSF-initiated Session Locking (FTA_SSL.1.1)	SL.1 The TSF shall lock an interactive session after an administrator-defined time interval of user activity by clearing or overwriting display devices, making the current contents unreadable and disabling any activity of the user's data access/display devices other than unlocking the session.
TSF-initiated Session Unlocking (FTA_SSL.1.2)	SL.2 The TSF shall require that prior to unlocking an interactive session the user must be successfully re-authenticated.

Table 7-7 SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
User Initiated Session Locking (FTA_SSL.2.1)	SL.3 The TSF shall allow user-initiated locking of the user's own interactive session by clearing or overwriting display devices, making the current contents unreadable and disabling any activity of the user's data access/display devices other than unlocking the session.
User Initiated Session Unlocking (FTA_SSL.2.2)	SL.4 The TSF shall require that prior to unlocking a user's interactive session, the user must be successfully re-authenticated.
TOE Session Establishment (FTA_TSE.1)	IA.1 The product shall require users to identify and successfully authenticate themselves, using a user name and a password, before performing any other actions
Inter-TSF Trusted Channel (FTP_ITC.1)	SC.7, SC.8 Communication channels provided by the TSF between itself and a remote trusted IT product must be logically distinct from other communications channels and must provide assured identification of the end points and protection of the channel data from modification or disclosure.
Trusted Path (FTP_TRP.1)	SC.9, TPath.1, TPath.2, TPath.3 Communication channels provided by the TSF between itself and remote or local users must be logically distinct from other communications channels and must provide assured identification of the end points and protection of the channel data from modification or disclosure. Also, the trusted path is required in order for a user to perform important security related functions.

- a. FAU_GEN.1.1 implicitly includes the requirement not to store password information in the audit trail as required by IT SF Audit.15.
- b. Supplying a new password is stated in ITSF IA.11, and it is the process through which a user enters a new password that enforces the construction of the password and hence the probability of guessing the correct password.

7.4.2 Justification for Compliance of Assurance Measures

Section 6.3 shows that all assurance requirements are met by an appropriate assurance measure.

The Security Functional Requirements outlined in section 7.4.1 are all met within the design of the Solaris 10 11/06 Trusted Extensions operating environment. Tests have been developed and will be conducted which confirm that all of the TOE security functional requirements are met.

7.5 PP Claims and Rationale

7.5.1 PP Reference

The TOE meets all of the requirements of the Controlled Access Protection Profile which is defined in [CAPP], the Labeled Security Protection Profile which is defined in [LSPP], and the Role Based Access Control Protection Profile which is defined in [RBAC].

7.5.2 PP Tailoring

The security functional requirements for the TOE are as defined in [CAPP], [LSPP], and [RBAC] with refinements as necessary and appropriate for a ST. These refinements are detailed in section 5.1.1.

7.5.3 PP Additions

There are a total of seven (7) additional security functional requirements for the TOE beyond those defined in [RBAC], [CAPP], and [LSPP] as follows: FDP_UCT.1; FDP_UIT.1; FMT_SMF.1; FTA_SSL.1; FTS_SSL.2; FTP_ITC.1 and FTP_TRP.1. These additional requirements are detailed in section 5.2.

There is one additional security requirement for the IT environment which is detailed in **section 5.5**. This relates to the requirements placed on the SC or OpenBoot PROM in support of protecting the server/workstation in the environment.

There are no additional TOE security objectives to those contained in [CAPP], [LSPP], and [RBAC]. The security objectives for the TOE environment in this ST may be regarded as additional to those contained in [CAPP], [LSPP], and [RBAC], although they are deemed to be broadly equivalent, and refined due to the specific environment assumed for the Trusted Extensions product.

7.5.4 PP Rationale

The objectives used in this ST are derived from [CAPP], [LSPP], and [RBAC]. The differences are minor and result from refinements appropriate to a Security Target where a specific product and the assumed environment are being described. The SFRs used in this ST are derived from [CAPP], [LSPP], and [RBAC], and have been refined as required for inclusion in a ST.

The rationale presented in this document describing why the SFRs are appropriate to meet the security objectives has been taken from [CAPP], [LSPP], and [RBAC] also. Because of the similarities between the objectives and SFRs contained in this ST and in [CAPP], [LSPP], and [RBAC], the justification provided in [CAPP], [LSPP], and [RBAC] is also appropriate for this ST.

This Page Intentionally Left Blank

Appendix A



A 1.1 Platform 1 Configurations

<i>Platform Specification</i>	Server E3500	Server E4500	Server E5500	Server E6500	Server E10K	Server E450	Server E420R	Server E250	Server E220R
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment								
<i>CPUs</i>	1-8	1-14	1-14	1-30	4-64	1-4	1-4	1-2	1-2
<i>Processor</i>	UltraSPARC II					UltraSPARC II with onboard e-cache			
<i>Clock speeds</i>	167; 250, 336, 400, 464, 500 or 650 MHz					250, 300, 400, 450 or 480 Mhz			
<i>I/O Slots (SBus/PCI)</i>	2 SBus	3 SBus	3 SBus	2 SBus 2 PCI	4 SBus 6 PCI	10 PCI	4 PCI	4 PCI	4 PCI
<i>Maximum Memory</i>	2 GB	2 GB	2 GB	56 GB	64 GB	4 GB	4 GB	2 GB	2 GB
<i>Max Storage</i>	n/a	144 GB	144 GB	72.8 GB	2 TB	730 GB	72.8 GB	216 GB	72.8 GB

<i>Platform Specification</i>	Ultrasparc 30	Ultrasparc 60	Ultrasparc 80	Ultrasparc 450	SunFire V100 ¹	Sunblade 100	Netra X1
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment						
<i>CPUs</i>	1	1-2	1-4	1-4	1	1	1
<i>Processor</i>	UltraSPARC-IIe						
<i>Clock speeds</i>	250, 300, 450 or 500 MHz						
<i>I/O Slots (SBus/PCI)</i>	4 PCI	4 PCI	4 PCI	10 PCI	2 USB	2 PCI	2 USB
<i>Maximum Memory</i>	2 GB	2 GB	4 GB	4 GB	2 GB	2 GB	2 GB
<i>Max Storage</i>	18 GB	72 GB	72 GB	730 GB	40 GB	30GB	80 GB



A.1.1 Platform 1 Configurations - Continued

<i>Platform Specification</i>	SunBlade 1000	SunBlade 2000	Netra 20	SunFire V280R	SunFire V480	SunFire V880	SunFire V880z
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment						
<i>CPUs</i>	1-2	1-2	1-2	1-2	2 or 4	2 - 8	1-6
<i>Processor</i>	UltraSPARC III Cu 8MHz Cache						
<i>Clock speeds</i>	600Mhz, 750Mhz, 900MHz, 1015MHz, 1050MHz & 1200MHz						
<i>I/O Slots (SBus/PCI)</i>	4 PCI	4 PCI	4 PCI	4 PCI	6 PCI	9 PCI	9 PCI
<i>Maximum Memory</i>	8 GB	8 GB	8 GB	8 GB	32 GB	64 GB	48 GB
<i>Max Storage</i>	146 Gb	146 GB	146 GB	146 GB	3 TB	3 TB	73 TB

<i>Platform Specification</i>	SunFire V210	SunFire V240	Netra 240	SunFire V250	SunFire V440	Netra 440 Server	SunBlade 1500	SunBlade 2500
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment							
<i>CPUs</i>	1-2	1-2	1-2	1-2	1-2	1-2	1	1-2
<i>Processor</i>	UltraSPARC IIIi 8MHz Cache							
<i>Clock speeds</i>	900MHz, 1015MHz, 1050MHz, 1200MHz & 1.503 GHz							
<i>I/O Slots (SBus/PCI)</i>	1 PCI	3 PCI	2 PCI 1 SCSI	6 PCI	6 PCI	6 PCI	4 PCI	6 PCI
<i>Maximum Memory</i>	4 GB	8 GB	8 GB	8 GB	16 GB	16 GB	8 GB	16 GB
<i>Max Storage</i>	146 GB	292 GB	292 GB	292 GB	292 GB	292 GB	120 GB	146 GB

<i>Platform Specification</i>	SunFire V125	SunFire V215	SunFire V245	SunFire V445	Ultra 25 Workstation	Ultra 45 Workstation
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment					
<i>CPUs</i>	1	1-2	1-2	1-4	1	1-2
<i>Processor</i>	UltraSparc IIIi Processor, 1MB Level 2 Cache					
<i>Clock speeds</i>	1.0, 1.34, 1.6 GHz					
<i>I/O Slots (SBus/PCI)</i>	1 PCI	2 PCI	4 PCI	8 PCI	6 PCI	6
<i>Maximum Memory</i>	8 GB	16 GB	16 GB	32 GB	8 GB	16 GB
<i>Max Storage</i>	146 GB	146 GB	292 GB	2.9 TB	1 TB	1 TB



A.1.1 Platform 1 Configurations - Continued

<i>Platform Specification</i>	Netra CT810	Netra CT820	Ultra Sparc 5	Ultra Sparc 10	Ultra 3 Mobile
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment				
<i>CPUs</i>	1 (single processor only)				
<i>Processor</i>	UltraSparc Ili 512Kb L2 on-die cache				
<i>Clock speeds</i>	270, 300, 333, 360, 440, 550, or 650 Mhz				
<i>I/O Slots (SBus/PCI)</i>	6 PCI	18 cPSB	3 PCI	4PCI	0
<i>Maximum Memory</i>	4 GB	2 GB	512 MB	1 GB	2 GB
<i>Max Storage</i>	144 GB	80 GB	20 GB	40 GB	80 GB

<i>Platform Specification</i>	Sun Blade 150	Sun Fire B100s	SunFire V100¹	Sun Fire V120	Netra 120	Netra CT410
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment					
<i>CPUs</i>	1 (single processor only)					
<i>Processor</i>	UltraSparc Ili 512Kb L2 on-die cache					
<i>Clock speeds</i>	270, 300, 333, 360, 440, 550, or 650 Mhz					
<i>I/O Slots (SBus/PCI)</i>	3 PCI	0	0	1 PCI	1 PCI	2 PCI
<i>Maximum Memory</i>	2 GB	2 GB	2 GB	4 GB	4 GB	4 GB
<i>Max Storage</i>	40 GB	40 GB	80 GB	108 GB	72 GB	72 GB

<i>Platform Specification</i>	Sun Fire T1000 Server	Sun Fire T2000 Server	Netra T2000 Server	Netra CP3060 Blade
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment			
<i>CPUs</i>	1	1	1	1
<i>Processor</i>	UltraSPARC T1 Chip Multithreaded (CMT)			
<i>Clock speeds</i>	1.2 GHz is 8 core, 1.0 GHz are 4, 6 or 8-core 3 MB unified level 2 cache with ECC			
<i>I/O Slots (SBus/PCI)</i>	1 PCI	5 PCI	5 PCI	8 PCIe
<i>Maximum Memory</i>	32 GB	64 GB	32 GB	64 GB
<i>Max Storage</i>	160 GB	292 GB	146 GB	292 GB

1. SunFire V100 was available with the Sparc Ii and Ili processors



A 1.2 Platform 2 Configurations

<i>Platform Specification</i>	Netra 1280	SunFire V1280	Sun Fire 3800	Sun Fire 4800	Sun Fire 4810	Sun Fire 6800	Sun Fire 12K	Sun Fire 15K
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment							
<i>CPUs</i>	4-12	4-12	2-8	2-12		2-24	4-52	16-106
<i>Processor</i>	UltraSPARC III Cu							
<i>Clock speeds</i>	900 Mhz		900MHz, 1050MHz & 1200MHz					
<i>System Board (CPU) Slots</i>	N/A	N/A	2	3		6	9	18
<i>I/O Slots (SBus/PCI)</i>	6 PCI	6 PCI	12 cPCI	16 PCI or 8 cPCI		32 PCI or 16 cPCI	36 PCI	72 PCI
<i>I/O Channel Bandwidth</i>	24 GB per second per PCI/cPCI assembly							
<i>Maximum Memory per domain</i>	96GB	96GB	64 GB	96 GB		192 GB	288 GB	576 GB
<i>Max Storage (all SunFire data center servers support external storage)</i>	17.5 TB	17.5 TB	35 TB			77 TB	120 TB	250 TB
<i>Sustained System Bandwidth</i>	9.6 GB/sec						21.6 GB/sec	43.2 GB/sec

<i>Platform Specification</i>	SunFire V490	SunFire V890	SunFire 2900	SunFire 4900	SunFire 6900	SunFire E20K	SunFire E25K	
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions Operating Environment							
<i>CPUs</i>	2-4	1-8	4, 8 or 12	4-12	2-24	4-36	8-72	
<i>Processor</i>	UltraSPARC III Cu or UltraSPARC IV							
<i>Clock speeds</i>	UltraSPARC IV: 1050MHz, 1200MHz or 1350 MHz SPARC V9		UltraSPARC[tm] III Cu: 900MHz, 1050MHz or 1200MHz UltraSPARC IV: 1050MHz, 1200MHz or 1350MHz superscalar SPARC V9, ECC protected					
<i>System Board (CPU) Slots</i>	3	3	3	3	6	9	18	
<i>I/O Slots (SBus/PCI)</i>	6 PCI	9 PCI, 2 USB	6 PCI	16 PCI	32 PCI	32 PCI	72 PCI	
<i>I/O Channel Bandwidth</i>	N/A		31.2 GB/sec aggregate bandwidth			150 MHz Sun[tm] Fire-plane redundant 18X18 interconnect		
<i>Maximum Memory per domain</i>	32 GB	64 GB	96 GB	96 GB	192 GB	288 GB	576 GB	
<i>Max Storage (all SunFire data center servers support external storage)</i>	292 GB	1.72 TB	146 GB	146 GB	146 GB	120 TB	250 TB	
<i>Sustained System Bandwidth</i>	N/A		9.6 GB/sec			21.6 GB/sec	43.2 GB/sec	



A 1.3 Platform 3 Configurations

<i>Platform Specification</i>	SunFire V20z	SunFire V40z	Sun Java Workstation W1100	Sun Java Workstation W2100	Dell PowerEdge 6000 Workstation
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions x86 Operating Environment				
<i>CPUs</i>	1-2	2-4	1	2	1-4
<i>Processor</i>	AMD-64 200 Series	AMD Opteron 800	AMD-64 100	AMD-64 200 Series	Intel(r) Xeon(tm)
<i>Clock speeds</i>	1.6GHz, 1.8GHz, 2.2GHz, 2.4GHz, 2.6GHz	1.8GHz, 2.2GHz, 2.4GHz, 2.6GHz	1.44Ghz, 1.46Ghz, 1.48Ghz, 1.50Ghz	2.44Ghz, 2.46Ghz, 2.48Ghz, 2.50Ghz	1.8Ghz
<i>I/O Slots (SBus/PCI)</i>	2 PCI	7 PCI	5 PCI, 1 AGP	5 PCI, 1 AGP	2 PCI
<i>Maximum Memory</i>	16 GB	32 GB	8 GB	16 GB	2 GB
<i>Max Storage (all SunFire data center servers support external storage)</i>	73 GB	1.8 TB	80 GB	146 GB	N/A

<i>Platform Specification</i>	SunFire x2100	SunFire x2100 M2	SunFire x2200 M2	SunFire x4100 / 4100 M2	SunFire x4200 / x4200 M2
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions x86 Operating Environment				
<i>CPUs</i>	1	1	1-2	1-2	1-2
<i>Processor</i>	AMD-64 100 Series	AMD dual core model 1200	AMD dual core 2000 series	AMD-64 200 / 2000 Series	AMD-64 200 / 2000 Series
<i>Clock speeds</i>	2.0, 2.4, 2.6, 2.8, 3.0 Ghz	1.8, 2.2, 2.6 GHz	1.8, 2.2, 2.6, 2.8 GHz	2.0GHz, 2.2GHz, 2.4GHz, 2.6GHz, 2.8GHz	2.0GHz, 2.2GHz, 2.4GHz, 2.6GHz, 2.8GHz
<i>I/O Slots (SBus/PCI)</i>	1 PCIe	1 PCIe	2 PCIe	2 PCI	5 PCI
<i>Maximum Memory</i>	8 GB	8 GB	32 GB	32 GB	32 GB
<i>Max Storage (all SunFire data center servers support external storage)</i>	1 TB	1 TB	1 TB	1 TB	500 GB



A.1.3 Platform 3 Configurations - Continued

<i>Platform Specification</i>	SunFire x4500	SunFire x4600	SunFire x4600 M2	Ultra 20 Workstation	Ultra 20 M2 Workstation
<i>Operating Environment</i>	Solaris 10 11/06 with Trusted Extensions x86 Operating Environment				
<i>CPUs</i>	1-2	4 or 8	4 or 8	1	1
<i>Processor</i>	AMD Opteron, Model 285	AMD Opteron 800 Series	AMD Opteron 8000 Series	AMD-64 100 Series	AMD Opteron 1200 Series
<i>Clock speeds</i>	2.6 GHz (95Watt)	2.6, 2.8 GHz	2.6, 2.8 GHz	1.8, 2.2 and 2.6GHz	1.8, 2.2, 2.6, and 2.8GHz
<i>I/O Slots (SBus/PCI)</i>	2 PCI	6 PCIe, 2 PCIx		6 PCI	6 PCI
<i>Maximum Memory</i>	16 GB	64 GB	128 GB	8 GB	8 GB
<i>Max Storage (all SunFire data center servers support external storage)</i>	24 TB	2 TB	2TB	500 GB	1 TB