Security Target for Oracle® Solaris 11.1

March 2014
Version 2

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Security Target for Oracle Solaris 11.1
Version 2

Author: Oracle Corporation

Contributors: Corsec Security, Inc.

Table of Contents

1 Introduction 1

Purpose 1
Security Target and TOE References 2
Product Overview 2
TOE Overview 5
TOE Description 7

2 Conformance Claims 11

3 Security Problem 13

Threats to Security 13
Organizational Security Policies 15
Assumptions 15

4 Security Objectives 17

Security Objectives for the TOE 17
Security Objectives for the Operational Environment 19

5 Extended Components 21

Extended TOE Security Functional 21
Extended TOE Security Assurance Components 26

6 Security Requirements 27

Conventions 27
Security Functional Requirements 27
Security Assurance Requirements 64

7 TOE Summary Specification 66

TOE Security Functionality 66

8 Rationale 85

Conformance Claims Rationale 85
Security Objectives Rationale 85
Rationale for Extended Security Functional Requirements 98
Rationale for Extended TOE Security Assurance Requirements 99

Security Requirements Rationale..... 99

A Glossary.....116

Acronyms..... 116

CHAPTER

1 Introduction

This chapter identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Oracle Solaris 11.1 SRU5.5, and will hereafter be referred to as the TOE throughout this document. The TOE is a highly configurable UNIX-based operating system that is optimized to quickly and securely deploy services in traditional enterprise data centers and large scale internet (or cloud) environments. It includes services such as resource management and network virtualization in order to provide an optimal performance with low overhead in both physical and virtualized environments. Solaris 11.1 SRU5.5 provides a sophisticated security system that controls the way users access files, protect system databases, and use system resources. Key high-level security services of Solaris 11.1 SRU5.5 include kernel protection, login protection, and data protection.

Purpose

This ST is divided into nine chapters, as follows:

- Introduction (Chapter 1) – Provides a brief summary of the ST contents and describes the organization of other chapters within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Chapter 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and EAL package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Chapter 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Chapter 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Chapter 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Chapter 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Chapter 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.

- Rationale (Chapter 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronym (A Glossary) – Defines the acronyms and terminology used within this ST.

Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Oracle Corporation Solaris 11.1 Security Target
ST Version	Version 2
ST Author	Corsec Security, Inc.
ST Publication Date	3/21/2014
TOE Reference	Oracle Solaris 11.1 SRU5.5
FIPS[1] 140-2 Status	Level 1, Validated crypto module, Certificate Numbers 1051, 2061 and 2077

Product Overview

Oracle Solaris 11.1 SRU5.5 is a highly configurable UNIX-based operating system that is optimized to quickly and securely deploy services in traditional enterprise data centers, large scale cloud environments and small personal desktop use. The operating system includes services such as hardware resource management and provides services for application software in order to provide optimal performance with low overhead. The operating system is an intermediary between application programs and computer resources. It is responsible for managing processes, processor time, and storage allocation to allow operation of processes and application software.

Solaris 11.1 SRU5.5 can be installed on either x86 or SPARC[2] hardware architectures or run in a virtualized environment. It allows one or more processors and multiple hardware peripheral and storage devices to be accessed by multiple users in order to meet user requirements.

Upon a successful log in to the Solaris 11.1 SRU5.5 operating system, users and administrators are granted access to all functions of the operating system for which they are granted privileges. This includes starting and stopping processes and applications, reading or writing files, and issuing operating system commands in the shell. The operating system enforces the security policy configured by administrators to protect data and ensures all activities that users can perform on the operating system are monitored and restricted as needed. All data that flow through the Solaris 11.1 SRU5.5 operating system is governed by the security policy set by administrators. The operating system can associate all data, or named objects, with a description of access rights. Per the security policy, the operating system enforces access to named objects.

[1] FIPS – Federal Information Processing Standard
[2] SPARC – Scalabale Processor Architecture

Solaris 11.1 SRU5.5 utilizes the GNU[3] GNOME[4] as its desktop environment. GNOME includes a simple graphical user interface (GUI) that runs on top of the Solaris 11.1 SRU5.5 operating system. In addition to GNOME as the user interface, Solaris 11.1 SRU5.5 is accessible through use of a command line interface (CLI) in order to perform administrative tasks. The CLI can also be accessed remotely. All functions of the operating system are accessible to the user through these two interfaces per the security policy.

Solaris 11.1 SRU5.5 provides a suite of technologies and applications that create an operating system with optimal performance. Solaris 11.1 SRU5.5 includes key technologies such as zones, ZFS[5] file system, Image Packaging System (IPS), multiple boot environments, trusted extensions, and cryptographic framework each of which is explained below.

Zones

A zone is a virtualized Operating System (OS) environment created within a single instance of the Oracle Solaris OS. The Oracle Solaris zones consist of software partitioning technology, which provide a means of virtualizing OS services to create an isolated environment for running applications. Zones provide a complete runtime environment for applications. The isolated environment prevents processes that are running in one zone from monitoring or affecting processes that are running in other zones.

Zones establish boundaries for resource consumption that can be expanded to adapt to changing processing requirements of the application running in the zone. Zones also establish namespace and security boundaries.

Zones in Solaris 11.1 SRU5.5 also allow Solaris 10 applications to run unmodified in the secure environment. Older applications automatically take advantage of the enhancements made to the kernel and utilize the newer technologies available to Solaris 11.1 SRU5.5.

ZFS File System

Solaris 11.1 SRU5.5 utilizes the ZFS file system, which provides a unique file system that is robust, scalable, and easily administered. ZFS uses the concept of storage pools to manage physical storage. Traditionally, systems use a single physical device and then a volume manager to provide a representation of a single device in order for file systems to take advantage of multiple devices.

ZFS eliminates the need for volume management. Instead of creating virtualized volumes, ZFS aggregates devices into a storage pool. The storage pool describes the physical characteristics of the storage (device layout, data redundancy, etc) and acts as a data store from which file systems can be created. While using ZFS, file systems are not constrained to individual devices and allows for sharing of physical disk space from all file systems in the pool. The size of the file system does not need to be predefined, as file systems grow automatically within the disk space allocated to the storage pool. When new storage is added, all file systems within the pool can immediately use the additional disk space.

With ZFS, all data and metadata is verified by a checksum algorithm that administrators can configure. All checksum verification and data recovery are performed at the file

[3] GNU stands for "GNU's not Unix". It is a Unix-like operating system developed by the GNU project.
[4] GNOME – GNU Network Object Model Environment.
[5] ZFS – Zettabyte File System

system layer, and are transparent to applications. In addition, ZFS provides for self-healing data. ZFS supports storage pools with varying levels of data redundancy. When a bad data block is detected, ZFS fetches the correct data from another redundant copy and repairs the bad data, replacing it with the correct data. The other key settable native properties of ZFS include compression, deduplication and encryption.

Other File Systems

ZFS is the default file system in Solaris 11.1 SRU5.5. The other file systems supported by Solaris 11 include:

- Network File System (NFSv4), a network based file system.
- UNIX File System (UFS), a legacy UNIX file system
- CD-ROM[6] File Systems
- PCFS[7] for DOS[8]-formatted disks that are written for DOS-based computers
- UDFS[9] for DVD[10] reading and writing

Image Packaging System

Image Packaging System is a new network based package management system. It provides a framework for complete software lifecycle management including installation, upgrade, and removal of software packages. Integrated with the ZFS file system, IPS ensures a safe system upgrade with ZFS Boot Environments by applying system updates to a clone of other file systems. Full cryptographic signature support is present to ensure end-to-end package and catalog integrity.

Boot Environment

Solaris 11.1 SRU5.5 provides the *beadm* utility to administer multiple bootable instances of the Solaris 11.1 SRU5.5 operating system images (boot environments) and any other application software packages installed onto said images. Administrators can maintain multiple boot environments and each boot environment can contain different installed versions of the software. Multiple boot environments reduce risks when updating software since administrators can create backup boot environments before making any software updates to the TOE. The creation of backup environments can be automatic as well as administrator initiated.

Trusted Extensions

Trusted Extensions (TX) defines and implements a labeled security policy. Access to data is controlled by special security tags, called labels. Labels are assigned to users, processes, and objects such as files and directories. These labels impose the Multilevel Confidentiality Information Flow Control Policy in addition to UNIX permissions, or Discretionary Access Control (DAC).

Cryptographic Framework

The TOE includes the Cryptographic Framework feature and the Key Management Feature (KMF) to provide central repositories for cryptographic services and key management in order for hardware, software, and end users to have access to optimized algorithms. The Cryptographic Framework provides cryptographic services to users and applications through individual commands, a user-level programming interface, a

[6] CD-ROM – Compact Disk – Read Only Memory
[7] PCFS – Personal Computer File System
[8] DOS- Disk Operating System
[9] UDFS – Universal Disk Format
[10] DVD – Digital Versatile Disc

kernel-level programming interface, a user-level cryptographic framework and a kernel-level cryptographic framework. KMF provides tools for centrally managing public key objects and public/private key pairs. All user-level software within the TOE requiring cryptographic services makes use of the consumer API[11] which is based on RSA[12] PKCS[13] #11[14].

Network Services

In addition to the key technologies above, Solaris 11.1 SRU5.5 includes a variety of network services to augment cloud-computing capabilities, which are explained below.

- Solaris 11.1 SRU5.5 provides NFS and NFS administrative capabilities. The NFS service enables any computer to access any other computer's file systems based on access controls configured by the administrator. The default NFS protocol utilized by Solaris 11.1 SRU5.5 is Transport Control Protocol (TCP).
- Solaris 11.1 SRU5.5 includes Solaris Secure Shell (SSH). The SSH daemon starts at boot time when network services are started. The default configuration of Solaris 11 only has SSH listening as a Network Service.
- Solaris 11.1 SRU5.5 includes Network Time Protocol (NTP) public domain software to set and maintain the system time through the use of a daemon. The daemon uses minimal system resources and the NTP client synchronizes automatically when it boots.

TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is Oracle Solaris 11.1 SRU5.5 operating system, typically configured in client-server architecture. The operating system can be installed through multiple methods as specified below:

- A LiveCD[15] image
- An interactive text installer
- The Oracle Solaris Automated Installer (AI) feature
- The Oracle Solaris SCI[16] Tool interactive system configuration tool
- The sysconfig(1M) command line system configuration tool

The TOE includes all the components and functionality described above in Chapter 1.

To interact with the TOE, users and administrators use the CLI or the GNOME GUI environment. All administrative configuration procedures are available through the CLI and GUI and all security policies are enforced using the two interfaces.

Figure 1 shows the details of a sample deployment configuration of the TOE.

[11] API – Application Programming Interface
[12] RSA – Rivest-Shamir-Adleman, a public-key encryption algorithm
[13] PKCS – Public Key Cryptography Standards
[14] RSA Security Inc. PKCS#11 Cryptographic Token Interface (Cryptoki)
[15] CD – Compact Disk
[16] SCI – System Configuration Interactive

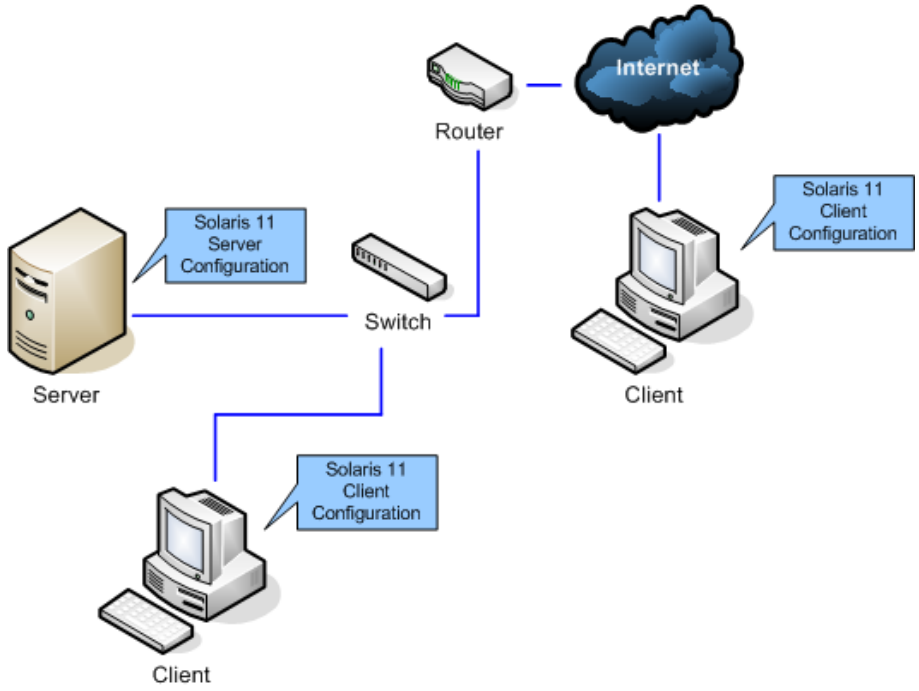


Figure 1 Sample Deployment Configuration of the TOE

The sample deployment shown in Figure 1 shows multiple instances of the TOE. All instances of the TOE are connected on a Local Area Network (LAN) provided by a network switch or a part of a Wide Area Network (WAN). One instance of the TOE is configured as a server connected to the LAN, and the other is a client configuration. A router provides an Internet gateway that allows restricted inbound and outbound connections. As part of the WAN, an instance of the TOE, configured as a client, communicates with a TOE in server configuration through a remote connection.

TOE Environment

The TOE environment consists of a hardware platform (either x86-based or SPARC-based system) on which the TOE can be installed. Table 2 specifies the minimum system requirements for the proper operation of the TOE when deployed on a hardware platform.

Table 2 TOE Minimum Requirements

Category	Requirement
Processors	Either x86 (64-bit), or SPARC architectures.
Memory	The minimum memory requirement is 512 MB.
Disk Space	The recommended size is at least 10 GB. A minimum of 4 GB is required.

The TOE environment also consists of an LDAP directory server, which is used as a naming repository to store information such as usernames, passwords and group memberships. In addition, the TOE needs cables and connectors that allow the TOE and environmental components to communicate with each other.

TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

Physical Scope

The TOE is the entire Solaris Operating System. The TOE does not include the user applications loaded to run on the operating system and the TOE does not include the hardware on which the OS is running.

Figure ***2*** illustrates the scope and the boundary of the overall solution and ties together all of the components of the TOE.

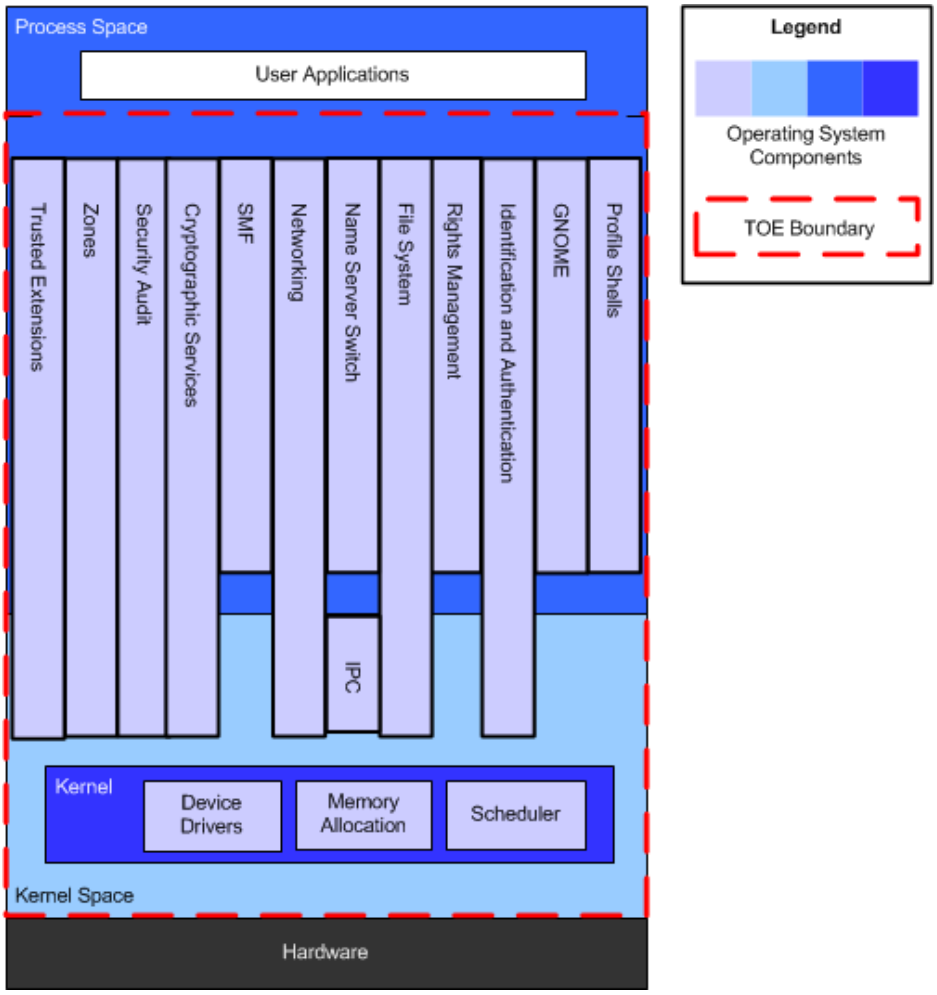


Figure 2 TOE Boundary

TOE Software

The TOE is the Solaris 11.1 SRU5.5 operating system that runs on either x86 (64-bit), or SPARC hardware architectures.

Guidance Documentation

Below are the TOE Guidance Documentation to install, configure, administer and maintain the TOE.

- Installing Oracle Solaris 11 Systems
- Creating and Administering Oracle Solaris 11 Boot Environments
- Adding and Updating Oracle Solaris 11 Software Packages
- Oracle Solaris 11 Installation Man Pages
- Oracle Solaris 11 Security Guidelines
- Oracle Solaris Administration: Security Services
- Trusted Extensions Configuration and Administration
- Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management

For a list of additional supporting guidance documentation see "Oracle Solaris 11.1 Guidance Supplement".

Logical Scope

The logical boundary of the TOE will be broken down into the following security classes, which are further, described in chapters 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Functional Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels

Security Audit

The TOE is capable of collecting extensive audit information about security related actions taken or attempted by its users. Audit records are generated when a specific auditable event occurs. Audit files can be stored locally or sent to a remote repository. Audit records may only be accessed (read-only) by authorized users of the TOE. The authorized users may specify specific classes into which a user may fall. These classes contain specific audit handling rules. The authorized users may then retrieve audit data based on user or subject identity, or by audit class, to name a few. The TOE will generate an alarm to notify an administrator if the audit trail exceeds the defined audit threshold or "soft limit" as configured by the administrator. In case of audit trail saturation, the TSF shall drop the records that cannot be written and count the dropped events.

Cryptographic Support

The TOE provides cryptographic functionality for authentication, data protection, and communications security purposes. This functionality comprises symmetric, asymmetric, hashing, random number generation, and message authentication code algorithms. In order to provide this functionality to various applications and operating system components in an elegant, optimized fashion, Oracle has included within the TOE the Solaris Cryptographic Framework. All crypto services in the evaluated configuration are provided by FIPS validated crypto modules. The FIPS 140-2 certificates of the crypto modules used by TOE are #1051, #2061 and #2077, and have been issued by the Cryptographic Module Validation Program (CMVP).

The Solaris Cryptographic Framework is utilized by SSH, Internet Protocol Security (IPsec)/ Internet Key Exchange (IKE), Kerberos and the Generic Security Services Application Programming Interface (GSSAPI), Simple Authentication and Security Layer (SASL), Lightweight Directory Access Protocol (LDAP), Pluggable Authentication Module (PAM), OpenSSL, the Java Cryptography Extension (JCE) framework, and a set of Solaris command line utilities.

User Data Protection

The TOE consists of three Access Control Policies and three Information Flow Control Policies. The Persistent Storage Object (PSO) Access Control Policy covers the access to TOE objects stored on non-volatile storage devices, such as flash memory, disk or ROM[17]. The Transient Storage Object (TSO) Access Control Policy covers the access to TOE objects stored on volatile storage devices, such as RAM[18]. The Zone Access Control Policy covers the access to TOE objects defined in the PSO and TSO Access Control Policies when zones are configured. Access to the TOE objects covered by these Security Function Policies (SFPs) is controlled based on the subject and object security attributes or zone security attributes as defined in the Zone Access Control Policy.

The Multilevel Confidentiality Information Flow Control Policy is a system-enforced mandatory access control (MAC) mechanism when TXs are enabled. It is an access control mechanism based on sensitivity labels. This policy also ensures that all exported and imported security attributes are properly labeled to show the sensitivity of the information. The Network Information Flow Control Policy will allow an IP[19] packet to be sent or received by a TOE subject such that it follows the specific rules laid out by the SFP. The Zone Information Flow Control Policy ensures that security attributes imported to the TOE are imported to the zone assigned to the users or process that initiate the importation.

Identification and Authentication

The TOE identification and authentication functionality enforces TOE users to successfully identify and authenticate to the TOE to access its functionality. However TOE users are able to select the language, desktop or console login, remote host for login, select fail safe login, and help for the login function prior to being identified and authenticated. Once successfully authenticated, the user will inherit the security attributes that were previously defined by an administrator for that user. A separate set of security attributes is also available to those users that are accessing the TOE remotely.

[17] ROM – Read Only Memory
[18] RAM – Random Access Memory
[19] IP – Internet Protocol

The TOE supports multiple authentication mechanisms via a pluggable framework (PAM) such as local files or a name service username and password, and Kerberos (or combinations of those), giving TOE users a convenient way to identify and authenticate themselves to the TOE.

Security Management

The TOE includes RBAC functionality (Chapter 7) to selectively grant administrative rights to users or roles as needed. The TOE authorized roles, or users have the ability to modify, query, and change the default values to all object security attributes. Each administrative user of the TOE will be assigned one or more roles for administrative use. Roles contain one or more rights profiles, privileges, and authorizations assigned, which will determine their level of access within the TOE. All object security attributes contain restrictive default values. It is up to the authorized roles, or users to modify the default values for each of the RBAC components listed in Chapter 7.

Protection of the TSF

The TOE provides reliable time stamps. The TSF has the capability to consistently interpret the security attributes specified in Persistent Storage Access Control Policy, Network Information Flow Control Policy, Zone Access Control Policy, and Zone Information Flow Control Policy when shared between the TSF and another trusted IT [20] product. When TX is enabled, the TSF provides the capability to consistently interpret label-related security attributes enforced by MAC SFP when shared between the TOE and another trusted IT product.

TOE Access

The TOE mitigates unauthorized user access by automatically locking a user session after an administrator predefined time interval of inactivity. The TOE also allows a user to manually lock their session. Locking the session will disable any activity of the user's TSF controlled data access and TSF controlled display devices other than unlocking the session. In order for an authorized user to regain access of a timed out session, the user must successfully re-authenticate with the credentials of the user owning the locked out session.

Trusted Path/Channels

The TSF provides cryptographically protected communication channels between itself and another IT trusted product. In its evaluated configuration, the TOE supports trusted communication channels for TCP and IP layer connections. The TOE supports SSH, IPsec, and Kerberos protocols to cryptographically secure the communications between itself and another trusted IT product that is logically distinct from other communication channels.

Product Physical/Logical Features and Functionality not included in the TOE

For a list of features/functionality that are not part of the evaluated configuration see "Oracle Solaris 11.1 Guidance Supplement".

[20] IT – Information Technology

CHAPTER

2 Conformance Claims

This chapter and Table 3 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Chapter 8. The Table 3 references the version of the Common Evaluation Methodology (CEM) and which interpretations apply to this evaluation.

Table 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP strict conformance; Parts 2 and 3 Interpretations of the CEM as of 2012/01/19 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	Conformant to the following BSI PP and extended packages: • OSPP - Operating System Protection Profile a. Version 2.0 b. 2010-06-01 c. BSI-CC-PP-0067 • AM - OSPP Extended Package – Advanced Management a. Version 2.0, b. 2010-05-28 c. BSI-CC-PP-0067 • EIA - OSPP Extended Package – Extended Identification and Authentication a. Version 2.0 b. 2010-05-28 c. BSI-CC-PP-0067 • LS - OSPP Extended Package – Labeled Security a. Version 2.0 b. 2010-05-28 c. BSI-CC-PP-0067 • VIRT - OSPP Extended Package – Virtualization a. Version 2.0 b. 2010-05-28 c. BSI-CC-PP-0067

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP strict conformance; Parts 2 and 3 Interpretations of the CEM as of 2012/01/19 were reviewed, and no interpretations apply to the claims made in this ST.
Evaluation Assurance Level	EAL4+ (Augmented with Flaw Remediation (ALC_FLR.3))

CHAPTER

3 Security Problem

This chapter describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

Threats to Security

This chapter identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The IT assets to be protected are:

- Persistent storage objects used to store user data and/or TSF data, where this data needs to be protected from any of the following operations:
  - Unauthorized read access
  - Unauthorized modification
  - Unauthorized deletion of the object
  - Unauthorized creation of new objects
  - Unauthorized management of object attributes
- Transient storage objects, including network data
- TSF functions and associated TSF data
- The resources managed by the TSF that are used to store the above-mentioned objects, including the metadata needed to manage these objects

The threat agents are external entities that potentially may attack the TOE. They are divided into three categories:

- External entities not authorized to access assets may attempt to access them either by masquerading as an authorized entity or by attempting to use TSF services without proper authorization
- External entities authorized to access certain assets may attempt to access other assets they are not authorized to either by misusing services they are allowed to use or by masquerading as a different external entity
- Untrusted subjects may attempt to access assets they are not authorized to either by misusing services they are allowed to use or by masquerading as a different subject

The TOE is a general-purpose, commercial-off-the-shelf operating system, which is generally seen as appropriate for a controlled environment where threat agents are assumed to have an enhanced-basic attack potential. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on

the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Chapter 4. Table 4 below lists the applicable threats.

Table 4 Threats

Name	Description
T.ACCESS.COMM	A threat agent might access a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system or masquerade as another remote trusted IT system.
T.ACCESS.TSFDATA	A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.
T.ACCESS.TSFFUNC	A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.
T.ACCESS.USERDATA	A threat agent might gain access to user data stored, processed, or transmitted by the TOE without being appropriately authorized according to the TOE security policy.
T.IA.MASQUERADE	A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA.USER	A threat agent might gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.
T.RESTRICT.NETTRAFFIC	A threat agent might get access to information or transmit information to other recipients via network communication channels without authorization for this communication attempt by the information flow control policy.
T.ROLE.SNOOP	An attacker might obtain the rights granted to a role that was delegated to another user.
T.ROLE.DELEGATE	An attacker might delegate rights granted to a role that he does not possess or that he is not allowed to delegate.
T.DATA_NOT_SEPARATED	The TOE might not adequately separate data on the basis of its sensitivity label, thereby allowing information to flow illicitly from or to users.
T.ACCESS.COMPENV	A threat agent might utilize or modify the runtime environment of other compartments in an unauthorized manner.
T.INFOFLOW.COMP	A threat agent might get access to information without authorization by the information flow control policy.
T.COMM.COMP	A threat agent might access the data communicated between compartments or between a compartment and an external entity to read or modify the transferred data.

Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 5 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 5 Organizational Security Policies

Name	Description
P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
P.APPROVE	Specific rights assigned to users and controlled by the TSF shall only be exercisable if approved by a second user.
P.CLEARANCE	The system must limit information flow between protected resources and authorized users based on whether the user's sensitivity label is appropriate for the labeled information.
P.I&A.REMOTE	Remote trusted IT systems shall be able to obtain identification and authentication decisions from the TOE based on credentials transmitted by a remote trusted IT system to the TOE.
P.LABELED_OUTPUT	The beginning and end of all paged, hardcopy output must be marked with sensitivity labels that properly represent the sensitivity label of the output.
P.RESOURCE_LABELS	All resources accessible by subjects and all subjects must have associated labels identifying the sensitivity levels of data contained therein.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.
P.USER_CLEARANCE	All users must have a clearance level identifying the maximum sensitivity levels of data they may access.

Assumptions

This chapter describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 Assumptions

Name	Description
A.AUTHUSER	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.
A.CONNECT	All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.
A.DETECT	Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
A.MANAGE	The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.PEER.FUNC	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.
A.PEER.MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

CHAPTER

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Chapter 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This chapter identifies the security objectives for the TOE and its supporting environment.

Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 Security Objectives for the TOE

Name	Description
O.AUDITING	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.COMP.IDENT	For each access request, the TOE is able to identify the compartment requesting to access resources, objects, or information.
O.COMP.INFO_FLOW_CTRL	The TOE will control information flow between compartments under the control of the TOE, based on security attributes of these compartments and potentially other TSF data (e.g., security attributes of objects). This information flow control policy must be able to allow the isolation of individual compartments from other compartments controlled by the TOE.

Name	Description
O.COMP.RESOURCE_ACCESS	The TOE will control access of compartments to objects and resources under its control based on: security attributes of the objects; security attributes of the compartment that attempts to access the object; and the type of access attempted. The rules that determine access may be based on the value of other TSF data. Access must be controlled down to individual compartments and objects.
O.CRYPTO.NET	The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.
O.DISCRETIONARY.ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.I&A	The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.
O.I&A.MULTIPLE	The TOE shall allow the concurrent use of multiple identification and authentication mechanisms implementing the identification and authentication policy.
O.I&A.REMOTE	The TOE shall allow remote trusted IT systems to transmit user credentials to the TOE. Using these credentials, the TOE shall perform a local identification and authentication policy decision, and then communicate this decision back to one or more trusted IT systems, based on the identification and authentication policy.
O.LS.CONFIDENTIALITY	The TOE will control information flow between entities and resources based on the sensitivity labels of users and resources.
O.LS.LABEL	The TOE will provide the capability to label all subjects, and all objects accessible by subjects, to restrict information flow based on the sensitivity labels.
O.LS.PRINT	The TOE will provide the capability to mark printed output with accurate labels based on the sensitivity label of the subject requesting the output.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.
O.NETWORK.FLOW	The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE

Name	Description
	and the TOE itself in accordance with its security policy.
O.ROLE.APPROVE	The TOE must prevent the execution of user actions allowed by a specific right until a second user with a different right approves this action.
O.ROLE.DELEGATE	The TOE must allow roles assigned to users for performing security-relevant management tasks to be delegated to other users in accordance with the security policy.
O.ROLE.MGMT	The TOE must allow security management actions based on roles to be assigned to different users.
O.SUBJECT.COM	The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.
O.TRUSTED_CHANNEL	The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.

Security Objectives for the Operational Environment

This chapter describes the environmental objectives.

IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment. The table references the Discretionary Access Control (DAC) policy of the TOE.

Table 8 IT Security Objectives

Name	Description
OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. Specifically, all network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system, as such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted; DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly; and users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their

Name	Description
	own data.
OE.INSTALL	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
OE.MAINTENANCE	Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
OE.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 (security) compromise is achieved.
OE.REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.
OE.TRUSTED.IT.SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

CHAPTER

5 Extended Components

This chapter defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Chapter 6.

Extended TOE Security Functional

This chapter specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE.

Table 9 Extended TOE Security Functional Requirements

Name	Description
FCS_RNG.1	Random number generation
FDP_RIP.3	Full residual information protection of resources
FIA_UAU.8	Authentication policy decisions
FIA_UID.3	Identification policy decisions
FIA_USB.2	Enhanced user-subject binding

Class FCS: Cryptographic Support

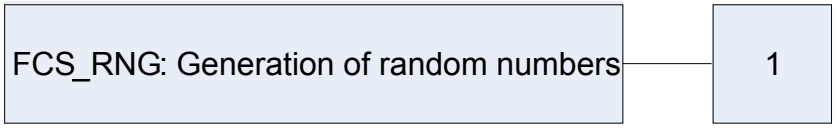
Families in this class address the requirements for functions to implement cryptographic functionality as defined in CC Part 2.

Family FCS_RNG: Generation of Random Numbers

Family Behavior

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component Leveling



FCS_RNG.1 Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

- There are no management activities foreseen.

Audit: FCS_RNG.1

- There are no actions defined to be auditable.

FCS_RNG.1	**Random number generation**
Hierarchical to:	**No other components**
FCS_RNG.1.1	The TSF shall provide a [selection: physical, non-physical true, deterministic, physical hybrid, deterministic hybrid] random number generator that implements: [assignment: list of security capabilities].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: a defined quality metric].
Dependencies:	**No dependencies**

Class FDP: User Data Protection

Families in this class specify requirements related to protecting user data as defined in CC Part 2.

Family FDP_RIP: Residual Information Protection

Family Behavior

This family addresses the need to ensure that any data contained in a resource is not available when the resource is de-allocated from one object and re-allocated to a different object. This family requires protection for any data contained in a resource that has been logically deleted or released, but may still be present within the TSF-controlled resource which in turn may be re-allocated to another object.

Components in this family address the requirements for implementing residual information protection as defined in CC Part 2. This chapter defines the extended components for the FDP_RIP family.

Component Leveling

The extended component FDP_RIP.3 is considered to be part of the FDP_RIP family.

FDP_RIP.3, Full residual information protection of resources, requires that the TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, de-allocation of the resource from] all subjects or users. FDP_RIP.3 is analog to FDP_RIP.2 except that it applies to the content of resources that are allocated to subjects or users.

Management: FDP_RIP.3

The following actions could be considered for the management functions in FMT:

- The choice of when to perform residual information protection (i.e. upon allocation or de-allocation) could be made configurable within the TOE.

Audit: FDP_RIP.3

- There are no auditable events foreseen.

FDP_RIP.3	**Full residual information protection of resources**
Hierarchical to:	**No other component**
FDP_RIP.3.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, de-allocation of the resource from] all subjects or users.
Dependencies:	**No dependencies**

Class FIA: Identification and Authentication

Families in this class address the requirements for functions to establish and verify a claimed user identity as defined in CC Part 2.

Family FIA_UAU: User Authentication

Family Behavior

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

This chapter defines the extended components for the FIA_UAU family.

Component Leveling

The extended FIA_UAU.8 component is considered to be part of the FIA_UAU family as defined in CC Part 2.

FIA_UAU.8 Authentication policy decisions, requires the TOE to perform authentication policy decisions that are communicated to other trusted IT systems.

Management: FIA_UAU.8

The following actions could be considered for the management functions in FMT:

- Management of rules for authentication policy decisions.

Audit: FIA_UAU.8

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism;
- Basic: All use of the authentication mechanism.

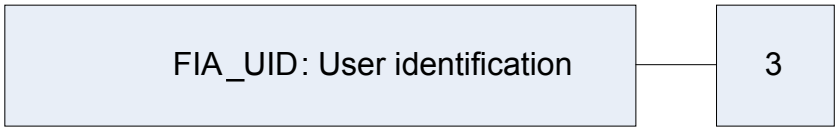
FIA_UAU.8	**Authentication policy decisions**
Hierarchical to:	**No other components**
FIA_UAU.8.1	The TSF shall accept an authentication request holding the user credentials from [assignment: list of trusted entities including other trusted IT products].
FIA_UAU.8.2	The TSF shall perform the authentication operation based on the transmitted user credentials according to [assignment: rules specifying how the authentication operation is performed].
FIA_UAU.8.3	The TSF shall transmit the result of the authentication operation to [assignment: list of entities including other trusted IT products] according to the [assignment: rules describing the selection process which entity or other trusted IT system receives the result].
Dependencies:	**FTP_ITC.1 Inter-TSF trusted channel**

Family FIA_UID: User Identification

Family Behavior

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

Component Leveling



The extended FIA_UID.3 component is considered to be part of the FIA_UID family as defined in CC Part 2.

FIA_UID.3	Identification policy decisions, requires the TOE to perform identification policy decisions that are communicated to other trusted IT systems.

Management: FIA_UID.3

The following actions could be considered for the management functions in FMT:

- Management of rules for authentication policy decisions.

Audit: FIA_UID.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the identification mechanism, including the user identity provided;
- Basic: All use of the identification mechanism, including the user identity provided.

FIA_UID.3	**Identification policy decisions**
Hierarchical to:	**No other components**
FIA_UID.3.1	The TSF shall accept an identification request holding the user credentials from [assignment: list of trusted entities including other trusted IT products].

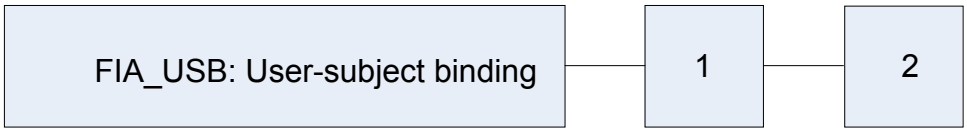
FIA_UID.3.2	The TSF shall perform the identification operation based on the transmitted user credentials according to [assignment: rules specifying how the identification operation is performed].
FIA_UID.3.3	The TSF shall transmit the result of the identification operation to [assignment: list of entities including other trusted IT products] according to the [assignment: rules describing the selection process which entity or other trusted IT system receives the result].
Dependencies:	**FTP_ITC.1 Inter-TSF trusted channel**

Family FIA_USB: User-subject binding

Family Behavior

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This family defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

Component Leveling



The extended FIA_USB.2 component is considered to be part of the FIA_USB family as defined in CC Part 2.

FIA_USB.2 Enhanced user-subject binding is analog to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes.

Management: FIA_USB.2

The following actions could be considered for the management functions in FMT:

- An authorized administrator can define default subject security attributes.
- An authorized administrator can change subject security attributes.

Audit: FIA_USB.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).
  Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

FIA_USB.2	**Enhanced user-subject binding**
Hierarchical to:	**FIA_USB.1 User-subject binding**
FIA_USB.2.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].
FIA_USB.2.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the

	behalf of users: [assignment: rules for the initial association of attributes].
FIA_USB.2.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].
FIA_USB.2.4	The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].
Dependencies:	**FIA_ATD.1 User-attribute definition**

Extended TOE Security Assurance Components

This Security Target does not define any extended assurance components.

CHAPTER

6 Security Requirements

This chapter defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Chapter 6.

Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the ST reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Assignments: Completed assignment statements are identified using [*italicized text within brackets*].
- Selections: Completed selection statements are identified using [underlined text within brackets].
- Refinements: Additions are identified using **bold text**; Removed text is stricken (Example: TSF Data).
- Iterations are identified by appending a suffix to the SFR identification. For example, FCS_CKM.1 (DSA) Cryptographic Key Generation would be one iteration of FCS_CKM.1 and FCS_CKM.1 (RSA) Cryptographic Key Generation would another.

Security Functional Requirements

This chapter specifies the SFRs for the TOE. This chapter organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓	✓	
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SEL.1	Selective audit	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			

Name	Description	S	A	R	I
FAU_STG.3	Action in case of possible data loss		✓	✓	
FAU_STG.3(Remote)	Action in case of possible data loss		✓	✓	
FAU_STG.4	Prevention of audit data loss	✓	✓		
FCS_CKM.1(DSA)	Cryptographic key generation	✓	✓	✓	✓
FCS_CKM.1(RSA)	Cryptographic key generation		✓	✓	✓
FCS_CKM.1(SYM)	Cryptographic key generation		✓	✓	✓
FCS_CKM.2(NET)	Cryptographic key distribution	✓	✓	✓	
FCS_CKM.4	Cryptographic key destruction	✓	✓		
FCS_COP.1(NET)	Cryptographic operation	✓	✓	✓	
FCS_RNG.1	Random number generation	✓	✓		
FDP_ACC.1(PSO)	Subset access control		✓		✓
FDP_ACC.1(TSO)	Subset access control		✓		✓
FDP_ACC.2(VIRT)	Complete access control		✓	✓	
FDP_ACF.1(PSO)	Security attribute based access control		✓		✓
FDP_ACF.1(TSO)	Security attribute based access control		✓		✓
FDP_ACF.1(VIRT)	Security attribute based access control		✓	✓	✓
FDP_ETC.2(LS)	Export of user data with security attributes		✓		✓
FDP_ETC.2(VIRT)	Export of user data with security attributes		✓	✓	✓
FDP_IFC.2(LS)	Complete information flow control		✓	✓	✓
FDP_IFC.2(NI)	Complete information flow control		✓		✓
FDP_IFC.2(VIRT)	Complete information flow control		✓	✓	✓
FDP_IFF.1(NI)	Simple security attributes	✓	✓		✓
FDP_IFF.1(VIRT)	Simple security attributes		✓	✓	✓
FDP_IFF.2(LS)	Hierarchical security attributes		✓	✓	
FDP_ITC.1(LS)	Import of user data without security attributes		✓	✓	
FDP_ITC.2	Import of user data with security attributes		✓		✓
FDP_ITC.2(LS)	Import of user data with security attributes		✓	✓	✓
FDP_ITC.2(VIRT)	Import of user data with security attributes		✓	✓	✓
FDP_RIP.2	Full residual information protection	✓			
FDP_RIP.3	Full residual information protection of resources	✓			
FIA_AFL.1	Authentication failure handling	✓	✓	✓	
FIA_ATD.1(EIA)	User attribute definition		✓	✓	✓
FIA_ATD.1(HU)	User attribute definition		✓	✓	✓
FIA_ATD.1(LS)	User attribute definition		✓		✓

Name	Description	S	A	R	I
FIA_ATD.1(TU)	User attribute definition		✓	✓	✓
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓	✓	
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UAU.8(EIA)	Authentication policy decisions		✓		
FIA_UID.1	Timing of identification		✓		
FIA_UID.2(VIRT)	User identification before any action			✓	
FIA_UID.3(EIA)	Identification policy decisions		✓		
FIA_USB.1(LS)	User-subject binding		✓	✓	
FIA_USB.2	Enhanced user-subject binding		✓		
FMT_MSA.1(LS)	Management of security attributes	✓	✓	✓	✓
FMT_MSA.1(PSO)	Management of object security attributes	✓	✓		✓
FMT_MSA.1(TSO)	Management of object security attributes	✓	✓		✓
FMT_MSA.1(VIRT-CACP)	Management of security attributes	✓	✓	✓	✓
FMT_MSA.1(VIRT-CIFCP)	Management of security attributes	✓	✓	✓	✓
FMT_MSA.3(LS)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(NI)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(PSO)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(TSO)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(VIRT-CACP)	Static attribute initialisation	✓	✓	✓	✓
FMT_MSA.3(VIRT-CIFCP)	Static attribute initialisation	✓	✓	✓	✓
FMT_MSA.4(PSO)	Security attribute value inheritance		✓	✓	
FMT_MTD.1(AE)	Management of TSF data	✓	✓		✓
FMT_MTD.1(AF)	Management of TSF data	✓	✓		✓
FMT_MTD.1(AM-AP)	Management of TSF data	✓	✓	✓	✓
FMT_MTD.1(AM-MA)	Management of TSF data	✓	✓	✓	✓
FMT_MTD.1(AM-MD)	Management of TSF data	✓	✓		✓
FMT_MTD.1(AM-MR)	Management of TSF data	✓	✓		✓
FMT_MTD.1(AS)	Management of TSF data	✓	✓		✓
FMT_MTD.1(AT)	Management of TSF data	✓	✓		✓
FMT_MTD.1(EIA)	Management of TSF data	✓	✓		✓
FMT_MTD.1(IAF)	Management of TSF data	✓	✓		✓

Name	Description	S	A	R	I
FMT_MTD.1(IAT)	Management of TSF data	✓	✓		✓
FMT_MTD.1(IAU)	Management of TSF data	✓	✓		✓
FMT_MTD.1(NI)	Management of TSF data	✓	✓		✓
FMT_MTD.1(VIRT-COMP)	Management of TSF data	✓	✓	✓	✓
FMT_REV.1(OBJ)	Revocation	✓	✓	✓	✓
FMT_REV.1(USR)	Revocation	✓	✓	✓	✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable time stamps				
FPT_TDC.1	Inter-TSF basic TSF data consistency		✓		✓
FPT_TDC.1(LS)	Inter-TSF basic TSF data consistency		✓		✓
FPT_TDC.1(VIRT)	Inter-TSF basic TSF data consistency		✓		✓
FTA_SSL.1	TSF-initiated session locking		✓	✓	
FTA_SSL.2	User-initiated locking		✓	✓	
FTP_ITC.1	Inter-TSF trusted channel	✓	✓	✓	

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

Security Audit

FAU_GEN.1 **Audit Data Generation**

Hierarchical to: **No other components.**

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

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

b) All auditable events for the [basic] level of audit; and

c) [All modifications to the set of events being audited;

d) All user authentication attempts;

e) All denied accesses to objects for which the access control policy defined in the OSPP base applies;

f) Explicit modifications of access rights to objects covered by the access control policies; and

g) *The events listed in Table 11*]

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

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

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

i. User identity (if applicable); and

ii. *The sensitivity labels of subjects, objects, or information involved (When TX is enabled)*]

Table 11 Auditable Events

Component	Event	Type
FAU_GEN.1	None	N/A
FAU_GEN.2	None	N/A
FAU_SAR.1	Reading of information from the audit records	Basic
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	Basic
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	Minimal
FAU_STG.1	None	N/A
FAU_STG.3	Actions taken due to exceeding of a threshold	Basic
FAU_STG.3 (Remote)	Actions taken due to network failure or timeouts	Basic
FAU_STG.4	Actions taken due to the audit storage failure	Basic
FCS_CKM.1 (DSA)	Cryptographic key generation	N/A
FCS_CKM.1 (RSA)	Cryptographic key generation	N/A
FCS_CKM.1 (SYM)	None	N/A
FCS_CKM.2 (NET)	Cryptographic key generation	N/A
FCS_CKM.4	None	N/A
FCS_COP.1 (NET)	None	N/A
FCS_RNG.1	None	N/A
FDP_ACC.1 (PSO)	None	N/A
FDP_ACC.1 (TSO)	None	N/A
FDP_ACC.2 (VIRT)	None	N/A
FDP_ACF.1 (PSO)	1. Successful requests to perform an operation on an object covered by the SFP 2. All requests to perform an operation on an object covered by the SFP	1. Minimal 2. Basic
FDP_ACF.1 (TSO)	1. Successful requests to perform an operation on an object covered by the SFP 2. All requests to perform an operation on an object covered by the SFP	1. Minimal 2. Basic

Component	Event	Type
FDP_ACF.1 (VIRT)	1. Successful requests to perform an operation on an object covered by the SFP 2. All requests to perform an operation on an object covered by the SFP	1. Minimal 2. Basic
FDP_ETC.2 (LS)	1. Successful export of information 2. All attempts to export information	1. Minimal 2. Basic
FDP_ETC.2 (VIRT)	1. Successful export of information 2. All attempts to export information	1. Minimal 2. Basic
FDP_IFC.2 (LS)	None	N/A
FDP_IFC.2 (NI)	None	N/A
FDP_IFC.2 (VIRT)	None	N/A
FDP_IFF.1 (NI)	1. Decisions to permit requested information flows 2. All decisions on requests for information flow	1. Minimal 2. Basic
FDP_IFF.1 (VIRT)	1. Decisions to permit requested information flows 2. All decisions on requests for information flow	1. Minimal 2. Basic
FDP_IFF.2 (LS)	1. Decisions to permit requested information flows 2. All decisions on requests for information flow	1. Minimal 2. Basic
FDP_ITC.1 (LS)	1. Successful import of user data, including any security attributes 2. All attempts to import user data, including any security attributes	1. Minimal 2. Basic
FDP_ITC.2	1. Successful import of user data, including any security attributes 2. All attempts to import user data, including any security attributes	1. Minimal 2. Basic
FDP_ITC.2 (LS)	1. Successful import of user data, including any security attributes 2. All attempts to import user data, including any security attributes	1. Minimal 2. Basic
FDP_ITC.2 (VIRT)	1. Successful import of user data, including any security attributes 2. All attempts to import user data, including any security attributes	1. Minimal 2. Basic
FDP_RIP.2	None	N/A
FDP_RIP.3	None	N/A

Component	Event	Type
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	Minimal
FIA_ATD.1 (EIA)	None	N/A
FIA_ATD.1 (HU)	None	N/A
FIA_ATD.1 (LS)	None	N/A
FIA_ATD.1 (TU)	None	N/A
FIA_SOS.1	1. Rejection by the TSF of any tested secret 2. Rejection or acceptance by the TSF of any tested secret	1. Minimal 2. Basic
FIA_UAU.1	1. Unsuccessful use of the authentication mechanism 2. All use of the authentication mechanism	1. Minimal 2. Basic
FIA_UAU.5	1. The final decision on authentication 2. The result of each activated mechanism together with the final decision.	1. Minimal 2. Basic
FIA_UAU.7	None	N/A
FIA_UAU.8 (EIA)	1. Unsuccessful use of the authentication mechanism 2. All use of the authentication mechanism	1. Minimal 2. Basic
FIA_UID.1	1. Unsuccessful use of the user identification mechanism, including the user identity provided 2. All use of the user identification mechanism, including the user identity provided	1. Minimal 2. Basic
FIA_UID.2 (VIRT)	1. Unsuccessful use of the user identification mechanism, including the user identity provided 2. All use of the user identification mechanism, including the user identity provided	1. Minimal 2. Basic
FIA_UID.3 (EIA)	1. Unsuccessful use of the identification mechanism, including the user identity provided 2. All use of the identification mechanism, including the user identity provided	1. Minimal 2. Basic

Component	Event	Type
FIA_USB.1 (LS)	1. Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject) 2. Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject)	1. Minimal 2. Basic
FIA_USB.2	1. Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject) 2. Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject)	1. Minimal 2. Basic
FMT_MSA.1 (LS)	All modifications of the values of security attributes	Basic
FMT_MSA.1 (PSO)	All modifications of the values of security attributes	Basic
FMT_MSA.1 (TSO)	All modifications of the values of security attributes	Basic
FMT_MSA.1 (VIRT-CACP)	All modifications of the values of security attributes	Basic
FMT_MSA.1 (VIRT-CIFCP)	All modifications of the values of security attributes	Basic
FMT_MSA.3 (LS)	1. Modifications of the default setting of permissive or restrictive rules 2. All modifications of the initial values of security attributes	1. Basic 2. Basic
FMT_MSA.3 (NI)	1. Modifications of the default setting of permissive or restrictive rules 2. All modifications of the initial values of security attributes	1. Basic 2. Basic
FMT_MSA.3 (PSO)	1. Modifications of the default setting of permissive or restrictive rules 2. All modifications of the initial values of security attributes	1. Basic 2. Basic
FMT_MSA.3 (TSO)	1. Modifications of the default setting of permissive or restrictive rules 2. All modifications of the initial values of security attributes	1. Basic 2. Basic
FMT_MSA.3 (VIRT-CACP)	1. Modifications of the default setting of permissive or restrictive rules 2. All modifications of the initial values of security attributes	1. Basic 2. Basic
FMT_MSA.3 (VIRT-CIFCP)	1. Modifications of the default setting of permissive or restrictive rules 2. All modifications of the initial values of security attributes	1. Basic 2. Basic

Component	Event	Type
FMT_MSA.4 (PSO)	Modifications of security attributes, possibly with the old and/or values of security attributes that were modified.	Basic
FMT_MTD.1 (AE)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AF)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AM-AP)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AM-MA)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AM-MD)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AM-MR)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AS)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (AT)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (EIA)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (IAF)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (IAT)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (IAU)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (NI)	All modifications to the values of TSF data.	Basic
FMT_MTD.1 (VIRT-COMP)	All modifications to the values of TSF data.	Basic
FMT_REV.1 (OBJ)	1. Unsuccessful revocation of security attributes 2. All attempts to revoke security attributes	1. Minimal 2. Basic
FMT_REV.1 (USR)	1. Unsuccessful revocation of security attributes 2. All attempts to revoke security attributes	1. Minimal 2. Basic
FMT_SMF.1	Use of the management functions.	Minimal
FMT_SMR.1	Modifications to the group of users that are part of a role	Minimal
FPT_STM.1	Changes to the time	Minimal
FPT_TDC.1	1. Successful use of TSF data consistency mechanisms. 2. Use of the TSF data consistency mechanisms. 3. Identification of which TSF data have been interpreted. 4. Detection of modified TSF data.	1. Minimal 2. Basic 3. Basic 4. Basic

Component	Event	Type
FPT_TDC.1 (LS)	1. Successful use of TSF data consistency mechanisms. 2. Use of the TSF data consistency mechanisms. 3. Identification of which TSF data have been interpreted. 4. Detection of modified TSF data.	1. Minimal 2. Basic 3. Basic 4. Basic
FPT_TDC.1 (VIRT)	1. Successful use of TSF data consistency mechanisms. 2. Use of the TSF data consistency mechanisms. 3. Identification of which TSF data have been interpreted. 4. Detection of modified TSF data.	1. Minimal 2. Basic 3. Basic 4. Basic
FTA_SSL.1	1. Locking of an interactive session by the session locking mechanism. 2. Successful unlocking of an interactive session. 3. Any attempts at unlocking an interactive session.	1. Minimal 2. Minimal 3. Basic
FTA_SSL.2	1. Locking of an interactive session by the session locking mechanism. 2. Successful unlocking of an interactive session. 3. Any attempts at unlocking an interactive session.	1. Minimal 2. Minimal 3. Basic
FTP_ITC.1	1. Failure of the trusted channel functions. 2. Identification of the initiator and target of failed trusted channel functions. 3. All attempted uses of the trusted channel functions. 4. Identification of the initiator and target of all trusted channel functions.	1. Minimal 2. Minimal 3. Basic 4. Basic

Dependencies: **FPT_STM.1 Reliable time stamps**

Application Note: Audit records are records generated by the audit daemon (*auditd*) and are not generalized to */var/adm* or */var/log*.

FAU_GEN.2 **User identity association**
Hierarchical to: **No other components.**
FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies: **FAU_GEN.1 Audit data generation**
FIA_UID.1 Timing of identification

FAU_SAR.1 **Audit review**
Hierarchical to: **No other components.**

FAU_SAR.1.1	The TSF shall provide [*users that are authorized to assume identified roles*] with the capability to read [*all* audit information] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	**FAU_GEN.1 Audit data generation**

Application Note: Authorized identified roles maps to the Administrator configured roles with the corresponding rights profile, authorizations and supplementary rights profile (if applicable). For additional information refer to Role-based Access Control (RBAC) Policy (Chapter 7).

FAU_SAR.2	**Restricted audit review**
Hierarchical to:	**No other components.**
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
Dependencies:	**FAU_SAR.1 Audit review**

FAU_SEL.1	**Selective audit**
Hierarchical to:	**No other components.**
FAU_SEL.1.1	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: [*a) Type of audit event;* b) Subject or user identity; *c) Outcome (success or failure) of the audit event;* *d) Named object identity;* *e) Subject sensitivity label (when TX is enabled); and* *f) Object sensitivity label (when TX is enabled)*]
Dependencies:	**FAU_GEN.1 Audit data generation** **FMT_MTD.1 Management of TSF data**

Application Note: TSF groups like event types together to form audit class. TSF can select the set of events to be audited based on the audit class.

FAU_STG.1	**Protected audit trail storage**
Hierarchical to:	**No other components.**
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.
Dependencies:	**FAU_GEN.1 Audit data generation**

FAU_STG.3	**Action in case of possible audit data loss**
Hierarchical to:	**No other components.**
FAU_STG.3.1	The TSF shall [*generate an alarm to the authorized administrator and write a message to the machine console*] if the audit trail exceeds [*the soft limit*] **or if any of the following** [***drops below the minimum free space percentage as configured by the administrator***] **is detected that may result in a loss of audit records.**
Dependencies:	**FAU_STG.1 Protected audit trail storage**

FAU_STG.3 (Remote) Action in case of possible audit data loss

Hierarchical to: **No other components.**

FAU_STG.3.1 The TSF shall [

- *connect to the next audit server in the list of audit servers specified after the administrator configured number of retries have been attempted;*
- *if connection to all audit servers fail, the list is tried again from beginning; and*
- *generates an alarm to the authorized administrator and writes a message to the machine console indicating failure at every unsuccessful attempt to connect to the server*]

~~if the audit trail exceeds [*the soft limit*]~~ **if any of the following [**

- ***if the host is unreachable due to connectivity failure; or***
- ***a timeout occurs while sending data*] is detected that may result in a loss of audit records.**

Dependencies: **FAU_STG.1 Protected audit trail storage**

FAU_STG.4 Prevention of audit data loss

Hierarchical to: **FAU_STG.3 Action in case of possible audit data loss**

FAU_STG.4.1 The TSF shall [ignore audited events] and [*count the dropped events*] if the audit trail is full.

Dependencies: **FAU_STG.1 Protected audit trail storage**

Cryptographic Support

FCS_CKM.1 (DSA) Cryptographic key generation

Hierarchical to: **No other components.**

FCS_CKM.1.1 The TSF shall generate **DSA**[21] cryptographic keys in accordance with a specified cryptographic key generation algorithm [*defined in US*[22] *NIST*[23] *FIPS PUB 186-3 appendix B.1*] and specified cryptographic key sizes: [

a) L=1024, N=160 bits;

b) DSA domain parameter generation for specified values for L and N];

that meet the following:

a) [*U.S. NIST FIPS PUB 186-3,*

b) *U.S. NIST FIPS PUB 186-2]*

Dependencies: **FCS_CKM.2 Cryptographic key distribution**
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1 (RSA) Cryptographic key generation

Hierarchical to: **No other components.**

FCS_CKM.1.1 The TSF shall generate **RSA** cryptographic keys in accordance with a specified cryptographic key generation algorithm [*defined in U.S. NIST FIPS PUB 186-3 appendix B.3*] and specified cryptographic key sizes: [

a) *1024 bits,*

b) *2048 bits,*

c) *4096 bits,*

d) *8192 bits*]

[21] DSA – Digital Signature Algorithm
[22] US – United States (of America)
[23] NIST – National Institute of Standards and Technology

that meet the following:
a) [*U.S. NIST FIPS PUB 186-3,*
b) *U.S. NIST FIPS PUB 186-2*].

Dependencies: **FCS_CKM.2 Cryptographic key distribution**
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1 (SYM) **Cryptographic key generation**
Hierarchical to: **No other components.**
FCS_CKM.1.1 The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [*capable of generating a random bit sequence*] and specified cryptographic key sizes: [
a) 128 bits, ***(AES)***[24]
b) 168 bits, ***(TDES)***[25]
c) 256 bits, ***(AES)***
d) *192 bits* ***(AES)***]
that meet the following: [
a) US NIST FIPS PUB [26]*197,*
b) US NIST SP[27] *800-67,*
c) US NIST SP 800-38A,
d) US ANSI[28] *X9.52]*

Dependencies: **FCS_CKM.2 Cryptographic key distribution**
FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2 (NET) **Cryptographic key distribution**
Hierarchical to: **No other components.**
FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with ~~a~~ **the following** specified cryptographic key distribution method ~~**[assignment:** ***cryptographic key distribution method*****]**~~ that meets the following: [
a) Diffie-Hellman key agreement method defined for the SSH protocol by RFC[29]4253;
b) Public [DSS] host key exchange defined for the SSH protocol by RFC4253;
c) Diffie-Hellman key agreement method defined for the IKE protocol by RFC2409;
d) RSA Key Exchange defined for the SSH protocol by RFC4432;
e) Diffie-Hellman key agreement method defined for GSSAPI-enabled SSH defined by RFC4462;
f) GSSAPI wrapping and unwrapping allowing the use of AES in ECB[30] *mode as defined in RFC 5649;*
g) *GSSAPI wrapping and unwrapping allowing the use TDES in CBC mode as defined in RFC 3217]*

[24] AES – Advanced Encryption Standard
[25] TDES – Triple Data Encryption Standard
[26] FIPS PUB – Federal Information Processing Standard Publication
[27] SP – Special Publication
[28] ANSI – American National Standards Institute
[29] RFC – Request For Comments
[30] ECB – Electronic Code Book

Dependencies:	**FCS_CKM.1 Cryptographic key generation** **FCS_CKM.4 Cryptographic key destruction**
FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	**No other components.**
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *of [zeroization]* that meets the following: *[vendor-specific zeroization]*.
Dependencies:	**FCS_CKM.1 Cryptographic key generation**
FCS_COP.1 (NET)	**Cryptographic operation**
Hierarchical to:	**No other components.**
FCS_COP.1.1	The TSF shall perform [*encryption, decryption, integrity verification, peer authentication*] in accordance with ~~**a specified**~~ **the following** cryptographic algorithm**s,** cryptographic key sizes ~~**that meet the following**~~ **and applicable standards: [** a) SSH allowing the use of TDES in CBC[31] mode with 168 bits key size, and HMAC-SHA[32]1, defined by RFC 4253; b) SSH allowing the use of AES in CBC or CTR[33] mode with 128 bits and 256 bits key size, and HMAC-SHA1defined by RFC 4253; *c) SSH allowing the use of TDES in CBC mode with 168 bits key size, and HMAC-SHA256, HMAC-SHA384, or HMAC-SHA512 defined by RFC 4253;* *d) SSH allowing the use of AES in CBC or CTR mode with 128 bits and 256 bits key size, and HMAC-SHA256, HMAC-SHA384, or HMAC-SHA512 defined by RFC 4253;* *e) IPsec with IKE allowing the use of AES in CBC, CCM, and GCM[34] mode with 128 bits, 192 bits, and 256 bits key size, and SHA1, SHA256, SHA384, SHA512, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, or HMAC-SHA512 defined by RFC 4301, RFC 4303, RFC 3602, RFC 2404, and RFC 4868;* *f) IPsec with IKE allowing the use of TDES in CBC mode with 168 bits key size, and SHA1, SHA256, SHA384, SHA512, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, or HMAC-SHA512 defined by RFC 4301, RFC 4303, RFC 3602, RFC 2404, and RFC 4868;* g) *GSSAPI wrapping and unwrapping allowing the use of AES in ECB mode as defined in RFC 5649;* h) *GSSAPI wrapping and unwrapping allowing the use TDES in CBC mode as defined in RFC 3217;* i) *Kerberos allowing TDES with 168 bits key size as defined in RFC 3961;* j) *Kerberos allowing AES with 128 bits or 256 bits key size as defined in RFC 3961;* k) *IPSEC with pre-shared keys allowing the use of AES in CTR mode with 128 bits and 256 bits key size, and SHA-1 defined by RFC 4301 and RFC 4303 and the use of HMAC-SHA1 defined by RFC 4302***]**.

[31] CBC – Cipher Block Chaining
[32] HMAC-SHA – Hash-based Message Authentication Code – Secure Hash Algorithm
[33] CTR – Counter
[34] GCM – Galios/Counter Mode

Dependencies:	**FCS_CKM.1 Cryptographic key generation** **FCS_CKM.4 Cryptographic key destruction**

FCS_RNG.1	**Random number generation**
Hierarchical to:	**No other components.**
FCS_RNG.1.1	The TSF shall provide a [deterministic] random number generator that implement: [*forward secrecy and backward secrecy*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [the FIPS 186-2 standard and thus *the requirements of functionality class K3 for a medium strength of function as defined in BSI AIS 20*].
Dependencies:	**No dependencies.**

User Data Protection

FDP_ACC.1 (PSO)	**Subset access control**
Hierarchical to:	**No other components.**
FDP_ACC.1.1	The TSF shall enforce the [*Persistent Storage Object Access Control Policy*] on [*a) Subjects*[35] *b) Objects* *i. Persistent Storage Objects of the following types: data sets, terminals, devices, volumes, consoles, operator commands, programs, file system objects (such as regular files, directories, symbolic links, character special files)* c) *Operations: create, delete, enable, disable, modify, read, write and execute*]
Dependencies:	**FDP_ACF.1 Security attribute based access control**

FDP_ACC.1 (TSO)	**Subset access control**
Hierarchical to:	**No other components.**
FDP_ACC.1.1	The TSF shall enforce the [*Transient Storage Object Access Control Policy*] on [*a) Subjects* *b) Objects: Transient Storage Objects of the following type "system V IPC*[36]*, POSIX IPC, signals, sockets and named pipes"* c) *Operations: all operations among subjects and objects covered by the Transient Storage Object Access Control Policy*]
Dependencies:	**FDP_ACF.1 Security attribute based access control**

FDP_ACC.2 (VIRT)	**Complete access control**
Hierarchical to:	**FDP_ACC.1 Subset access control**
FDP_ACC.2.1	The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Access Control Policy*] on [*a) Subjects:* ~~*compartments*~~ ***zones****;* *b) Objects:*

[35] Subjects – Subjects are processes (execution contexts). They may either be acting on behalf of an identified and authenticated user (or role), or acting on behalf of the system.
[36] IPC – Inter-process Communication

i. *Persistent Storage Objects of those assigned in FDP_ACC(PSO).1.1,b;*
ii. *Transient Storage Objects of those assigned in FDP_ACC(TSO).1.1,b;*
iii. *Objects of those assigned in FDP_IFC.2 (LS) (FDP_IFC.2.1,b (When TX is enabled));*
iv. *no additional objects***]**

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACF.1 (PSO) **Security attribute based access control**

Hierarchical to: **No other components.**

FDP_ACF.1.1 The TSF shall enforce the [*Persistent Storage Object Access Control Policy*] to objects based on the following: *[*

a) User identity and group memberships associated with a subject; and

b) The following access control attributes associated with an Object: An access control list defining access rights as read, write, execute or denied or permission bits].

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

IF the object has an explicit ACL[37], then:

i. *access granted to the object's owner is based on the user::rwx permissions;*
ii. *access granted to individuals specified in the ACL is based on the bitwise AND operation of the user:[specified]:rwx and mask:rwx permissions;*
iii. *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;*
iv. *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;*
v. *access granted to all other subjects is based on the object's other permissions;*

ELSE

i. *access granted to the object's owner is based on the object user rwx permissions;*
ii. *access granted to subjects who belong to the object's group is based on the object group rwx permissions;*
iii. *access granted to all other subjects is based on the object other rwx permissions*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*If a subject has an effective override privilege, the TSF shall authorize access of the*

[37] ACL – Access Control List

subject to any given object, even if such access is disallowed by FDP_ACF (PSO).1.2].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACF.1 (TSO) **Security attribute based access control**

Hierarchical to: **No other components.**

FDP_ACF.1.1 The TSF shall enforce the [*Transient Storage Object Access Control Policy*] to objects based on the following: [

a) User identity and group memberships associated with a subject; and

b) *The following access control attributes associated with an object: permission bits*].

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

a) access *granted to the object's owner is based on the object owner's identity and group membership*

i. if the effective user ID of the process matches the owner's user ID or creator's user ID in the data structure associated with the system V IPC object and the appropriate bit of the "user" portion of the data structure is set;

ii. if the effective group ID of the process matches the owner's group ID or creator's group ID in the data structure associated with the system V IPC object and the appropriate bit of the" group" portion of the data structure is set; or

iii. if the appropriate bit of the "other" portion of the data structure is set

b) access *to objects in the kernel are controlled by access to the interfaces that are provided by kernel*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*If a subject has an effective override privilege, the TSF shall authorize access of the subject to any given object, even if such access is disallowed by FDP_ACF (TSO).1.2*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACF.1 (VIRT) **Security attribute based access control**

The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Access Control Policy*] to objects based on the following: [

a) Subject security attributes:

i. zone ID[38]*;*

ii. IP type;

[38] ID – identifier

iii. *zone privileges*[39]*;*

b) *Object security attributes:*

i. *Data link (each exclusive-IP zone has its own data link(s));*

ii. *Process ID;*

iii. *File System zone mount point(s);*

c) *No additional SFP-relevant security attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Access of a ~~compartment~~ **zone** to an object is allowed when the requested mode of access is allowed for the ~~compartment~~ **zon**e by the ~~compartment~~ **zone** access control permission settings for that object.*]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*If a subject has an effective override privilege, the TSF shall authorize access of the subject to any given object, even if such access is disallowed by FDP_ACF (VIRT).1.2*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ETC.2 (LS) **Export of user data with security attributes**

Hierarchical to: **No other components.**

FDP_ETC.2.1 The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy*] when exporting labeled user data, controlled under the SFP(s), outside of the TOE.

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

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

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

a) *When data is exported in hardcopy form, each page shall be marked with a printed representation of the sensitivity label of the subject requesting the export of the page. By default, this marking shall appear on both the top and bottom of each printed page.*

b) *When the data is exported to a device, the security attributes shall be exported with the data using*

i. *the printable label that is assigned to the sensitivity label associated with the data by the authorized administrator.*

c) *When data is exported in hardcopy form, each page shall be marked with a printed representation of the sensitivity label of the object when it is known instead of subject's sensitivity label. By default, this marking shall appear on both the top and bottom of each printed page.]*

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]

[39] Privileges – A discrete right on a process in an Oracle Solaris system. Privileges offer a finer-grained control of processes than does root. Privileges are defined and enforced in the kernel.

FDP_ETC.2 (VIRT)	**Export of user data with security attributes**
Hierarchical to:	**No other components.**
FDP_ETC.2.1	The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Access Control Policy and* ~~*Compartment*~~ ***Zone*** *Information Flow Control Policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [*no additional exportation control rules*].
Dependencies:	**[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]**

FDP_IFC.2 (LS)	**Complete information flow control**
Hierarchical to:	**FDP_IFC.1 Subset information flow control**
FDP_IFC.2.1	The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy***]** on [*a) Subjects*[40] ***b)*** *Objects: data sets, terminals, volumes, consoles, operator commands, programs, devices (allocatable devices such as tape drives, diskette drives, CD-ROM and DVD devices, and audio devices; and not allocatable devices such as printers, workstations and serial lines when they are used as login device), file system objects (such as regular files, directories, symbolic links, character special files), network interfaces, windows*] and all operations that cause that information to flow ~~to and from subjects covered by the SFP~~ **among them**.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow ~~to and from any subject~~ **among untrusted subjects and named objects** in the TOE are covered by ~~an information flow control policy~~ **the Multilevel Confidentiality Information Flow Control Policy**.
Dependencies:	**FDP_IFF.1 Simple security attributes**

FDP_IFC.2 (NI)	**Complete information flow control**
Hierarchical to:	**FDP_IFC.1 Subset information flow control**
FDP_IFC.2.1	The TSF shall enforce the [*Network Information Flow Control Policy*] on [*a) Subjects:* *i. Unauthenticated external IT entities that send and receive information mediated by the TOE;* *ii. none that send and receive information mediated by the TOE* *b) Information:* *i. Network data routed through the TOE;*

[40] Subjects are processes (execution contexts). They may either be acting on behalf of an identified and authenticated user (or role), or acting on behalf of the system.

ii. no other information]
and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Dependencies: **FDP_IFF.1 Simple security attributes**

Application Note: This requirement (FDP_IFC.2 (NI)) covers the internet protocols specified in FDP_IFF (NI) .1.1b.

FDP_IFC.2 (VIRT) **Complete information flow control**
Hierarchical to: **FDP_IFC.1 Subset information flow control**
FDP_IFC.2.1 The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Information Flow Control Policy*] on [
a) Subjects:
i. ~~*Compartments*~~ ***Zones****;*
ii. External entities;
iii. No additional subjects
b) Information:
i. User data belonging to ~~*compartments*~~ ***zones****;*
ii. User data belonging to subjects outside of ~~*compartments*~~ ***zones****;*
iii. TSF data;
iv. No additional information]
and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Dependencies: **FDP_IFF.1 Simple security attributes**

FDP_IFF.1 (NI) **Simple security attributes**
Hierarchical to: **No other components.**
FDP_IFF.1.1 The TSF shall enforce the [*Network Information Flow Control Policy*] based on the following types of subject and information security attributes: [
a) Object security attribute: the logical or physical network interface through which the network data entered the TOE;
b) *TCP/IP [41] information security attributes:*
i. *Source and destination IP address,*
ii. *Source and destination TCP port number,*
iii. *Source and destination UDP port number,*
iv. *Network protocol of IP, IPv4, IPv6, TCP, UDP, ICMP[42], ARP[43], SCTP[44], IPsec*
v. *TCP header flags of SYN[45], ACK,* [46]
vi. *[no other attributes of an IP packet];*
c) *IEEE[47] 802.1Q VLAN[48] tag information security attributes:*

[41] TCP/IP – Transmission Control Protocol/Internet Protocol
[42] ICMP – Internet Control Message Protocol
[43] ARP – Address Resolution Protocol
[44] SCTP – Stream Control Transmission Protocol
[45] SYN – Synchronize
[46] ACK - Acknowledge

i. VLAN tag;

d) no other network data information security attributes]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*For TOE TCP/IP stacks configured for IP security, the TOE allows an IP packet to be sent or to be received by a subject if a rule described in FDP_IFF.1.3 applies and explicitly allows the packet flow.*]

FDP_IFF.1.3 The TSF shall enforce the [*following rules:*
Identification of network data using one or more of the following concepts:
a) Information security attribute matching;
b) Matching based on the state of a TCP connection,
Performing one or more of the following actions with identified network data:
a) Discard the network data without any further processing,
b) Allow the network data to be processed unaltered by the TOE according to the routing information maintained by the TOE;
c) *no other actions*]

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*no additional rules*]

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*no additional rules.*]

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1 (VIRT) **Simple security attributes**
Hierarchical to: **No other components.**

FDP_IFF.1.1 The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Information Flow Control Policy*] based on the following types of subject and information security attributes: [
a) Subject security attributes:
i. Zone IP address;
ii. Root sub-directory of file system in a zone;
iii. No other additional subject security attributes;
b) Information security attributes:
i. user data: assigned zone, ACL, permission bits;
ii. TSF data: assigned zone, ACL, permission bits;
iii. zone :file-mac-profile]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*information may freely flow within the assigned zone but may only flow between the zones through the defined network Application Programming Interfaces (APIs) as specified in FDP_IFF.1.5*].

FDP_IFF.1.3 The TSF shall enforce the [*Persistent Storage Object Access Control Policy, and Transient Storage Object Access Control Policy*].

[47] IEEE – Institute of Electrical and Electronics Engineers
[48] VLAN – Virtual Local Area Network

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*as defined in the file-mac-profile*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*information may not flow between zones unless network API calls are used and permission is explicitly provided in file-mac-profile*].

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_MSA.3 Static attribute initialisation

FDP_IFF.2 (LS) **Hierarchical security attributes**

Hierarchical to: **FDP_IFF.1 Simple security attributes**

FDP_IFF.2.1 The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy*] based on the following types of subject and ~~information~~ **object** security attributes: [

a) Subject security attributes:
- *i. Sensitivity label of the subject consisting of at least ~~8~~ **255** site-definable hierarchical levels and a set of ~~60~~ 2^{256} site definable non-hierarchical categories;*
- *ii. None*

b) Object security attributes:
- *i. The sensitivity label of the object consisting of at least ~~8~~ **255** site-definable hierarchical levels and a set of ~~60~~ 2^{256} site definable non-hierarchical categories;*
- *ii. None*]

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled ~~information~~ **object** via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [

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

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

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

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

FDP_IFF.2.4 The TSF shall explicitly authorise an information flow based on the following rules: [*the authorized identified roles with appropriate authorizations can move information between files at different levels*].

FDP_IFF.2.5 The TSF shall explicitly deny an information flow based on the following rules: [*objects that are supposed to have a security label but do not have a security label*.]

FDP_IFF.2.6 The TSF shall enforce the following relationships for any two valid information flow control security attributes:

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

the security attributes are incomparable~~; and~~ **with the following properties:**

i. **Sensitivity labels are equal if the hierarchical levels of both labels are equal and the non-hierarchical category sets are identical;**

ii. **Sensitivity label A is greater than sensitivity label B if the hierarchical level of A is greater than or equal to the hierarchical level of B, and the non-hierarchical category set of A is identical to or a superset of the non-hierarchical category set of B;**

iii. **Sensitivity labels are incomparable if they are not equal and neither label is greater than the other as defined in i and ii above;**

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

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

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_MSA.3 Static attribute initialization

Application Note1: TX supports 255 site-definable hierarchical levels called classifications and 256 site-definable non-hierarchical category bits called compartments.

Application Note2: The default policy is view and modify access of equal labels. This can be configured to be view access of dominated labels and modify access of equal labels.

FDP_ITC.1 (LS) **Import of user data without security attributes**
Hierarchical to: **No other components.**
FDP_ITC.1.1 The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy*] when importing **unlabeled** user data controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2 The TSF shall ignore any **label-related** security attributes associated with the **unlabeled** user data when imported from outside the TOE.
FDP_ITC.1.3 The TSF shall enforce the following rules when importing **unlabeled** user data controlled under the SFP from outside the TOE: [

a) The TSF shall allow the authorized administrator to allocate devices which contain unlabeled data within an administratively specified device label range;

b) no additional importation control rules.]

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.2 **Import of user data with security attributes**

Hierarchical to:	**No other components.**
FDP_ITC.2.1	The TSF shall enforce the [*Persistent Storage Access Control Policy, Network Information Flow Control Policy and no additional SFP(s)*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*no additional importation control rules*.]
Dependencies:	**[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency**

FDP_ITC.2 (LS)	**Import of user data with security attributes**
Hierarchical to:	**No other components.**
FDP_ITC.2.1	The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy*] when importing **labeled** user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the **label-related** security attributes associated with the imported **labeled** user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the **label-related** security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*a) Devices used to import data with security attributes shall unambiguously associate security labels with the corresponding data. Security labels consist of the following:* *i. Classification field;* *ii. Compartments field*]
Dependencies:	**[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency**

FDP_ITC.2 (VIRT)	**Import of user data with security attributes**
Hierarchical to:	**No other components.**
FDP_ITC.2.1	The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Access Control Policy and* ***Zone*** ~~*Compartment*~~ *Information Flow Control Policy*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*data that is imported to the zone is assigned to the zone and to users or process that initiates importation*].
Dependencies:	**[FDP_ACC.1 Subset access control, or** **FDP_IFC.1 Subset information flow control]** **[FTP_ITC.1 Inter-TSF trusted channel, or** **FTP_TRP.1 Trusted path]** **FPT_TDC.1 Inter-TSF basic TSF data consistency**

FDP_RIP.2	**Full residual information protection**
Hierarchical to:	**FDP_RIP.1 Subset residual information protection**
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] all objects.
Dependencies:	**No dependencies**

FDP_RIP.3	**Full residual information protection of resources**
Hierarchical to:	**No other component**
FDP_RIP.3.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] all subjects or users.
Dependencies:	**No dependencies**

Identification & Authentication

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	**No other components.**
FIA_AFL.1.1	The TSF shall detect when [*an administrator configurable number of*] **consecutive** unsuccessful authentication attempts **for the authentication methods [*passwords*]** occur related to [*all authentication events*].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [*lockout the user account*].
Dependencies:	**FIA_UAU.1 Timing of authentication**

FIA_ATD.1 (EIA)	**User attribute definition**
Hierarchical to:	**No other components.**
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users **for remote identification and authentication**: [*Kerberos:* *User identifier* *Password]*

Dependencies:	**No dependencies**

FIA_ATD.1 (HU)	**User attribute definition**
Hierarchical to:	**No other components.**
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual **human** users: [*a) User identifier;* *b) Group memberships;* *c) User password;* *d) Software token verification data* *e) Security roles;* *f) Rights Profiles;* *g) Privileges;* *h) Authorizations;* *i) Kerberos ticket lifespan;* *j) X.509 v3 certificates; and* *k) Indication of the authentication algorithm used by the IPsec, Kerberos v5, SASL, SSH*]
Dependencies:	**No dependencies**

FIA_ATD.1 (LS)	**User attribute definition**
Hierarchical to:	**No other components.**
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [*a) Sensitivity label]*
Dependencies:	**No dependencies**

Application Note: The user attributes associated with sensitivity labels are clearance and min_label. Clearances contains the maximum label at which a user can operate, they are the least upper bounds for sensitivity labels. Min_label contains the minimum label at which a user can log in.

FIA_ATD.1 (TU)	**User attribute definition**
Hierarchical to:	**No other components.**
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual **technical** users: [*a) the logical or physical network interface through which the network data entered the TOE;* *b) identity of the logical or physical external interface through which the user connected to the TOE;* *c) Source IP address;* *d) Destination IP address;* *e) Source port;* *f) Destination port*]
Dependencies:	**No dependencies**

FIA_SOS.1	**Verification of secrets**
Hierarchical to:	**No other components.**
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [*the following quality metric: the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20*[49]].
Dependencies:	**No dependencies**

[49] 2^-20: a defined quality metric

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	**No other components.**
FIA_UAU.1.1	The TSF shall allow [*a) the information flow covered by the Network Information Flow Control Policy;* *b) select language;* *c) select desktop or console login;* *d) select remote host for login;* *e) help for login function;* *f) select fail safe login]* on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	**FIA_UID.1 Timing of identification**
FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	**No other components.**
FIA_UAU.5.1	The TSF shall provide **the following authentication mechanisms** [*a) Authentication based on username, and password;* *b) Authentication based on software token verification data;* *c) Authentication based on digital certificates, and Kerberos tickets; and* *d) Public key authentication*] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the **following rules** [*a) Authentication based on username and password is performed for TOE-originated requests and credentials stored by the TSF;* *b) Authentication based on software token verification data is performed for TOE-originated requests;* *c) Authentication based on digital certificates, and Kerberos tickets is performed for TOE-originated requests; and* d) *Authentication based on Public key authentication is performed for TOE-originated requests*]
Dependencies:	**No dependencies**
FIA_UAU.7	**Protected authentication feedback**
Hierarchical to:	**No other components.**
FIA_UAU.7.1	The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.
Dependencies:	**FIA_UAU.1 Timing of authentication**
FIA_UAU.8 (EIA)	**Authentication Policy Decisions**
Hierarchical to:	**No other components.**
FIA_UAU.8.1	The TSF shall accept an authentication request holding the user credentials from [*Kerberos clients*].

FIA_UAU.8.2 The TSF shall perform the authentication operation based on the transmitted user credentials according to [*the verified principal name of the user in the Kerberos principal database*].

FIA_UAU.8.3 The TSF shall transmit the result of the authentication operation to [*Kerberos clients*] according to the [
the verified principal name of the user in the Kerberos principal database].

Dependencies: **FTP_ITC.1 Inter-TSF trusted channel**

FIA_UID.1 **Timing of identification**
Hierarchical to: **No other components.**
FIA_UID.1.1 The TSF shall allow [
a) Universal access preferences]
on behalf of the user to be performed before the user is identified.

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

Dependencies: **No dependencies**

FIA_UID.2 (VIRT) **User identification before any action**
Hierarchical to: **FIA_UID.1 Timing of Identification.**
FIA_UID.2.1 The TSF shall require each ~~**compartment**~~ **zone** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: **No dependencies**

FIA_UID.3 (EIA) **Identification policy decisions**
Hierarchical to: **No other components.**
FIA_UID.3.1 The TSF shall accept an authentication request holding the user credentials from [*Kerberos clients*].

FIA_UID.3.2 The TSF shall perform the identification operation based on the transmitted user credentials according to [*the verified principal name of the user in the Kerberos principal database*].

FIA_UID.3.3 The TSF shall transmit the result of the identification operation to [*Kerberos clients*] according to the [
the verified principal name of the user in the Kerberos principal database].

Dependencies: **FTP_ITC.1 Inter-TSF trusted channel**

FIA_USB.1 (LS) **User-subject binding**
Hierarchical to: **No other components**
FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [
a) *User sensitivity level that is used to enforce the Multilevel Confidentiality Information Flow Control Policy* ***which consists of***
i. Classification field, and
ii. Compartments field]

FIA_USB.1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [
a) The sensitivity label associated with a subject shall be within the clearance range of the user]

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*none*]

Dependencies: **FIA_ATD.1 User Attribute Definition**

FIA_USB.2 **Enhanced user-subject binding**

Hierarchical to: **FIA_USB.1 User-subject binding**

FIA_USB.2.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [

a) The user identity that is associated with auditable events

b) The user security attributes that are used to enforce the Persistent Storage Object Access Control Policy;

c) The user security attributes that are used to enforce the Transient Storage Object Access Control Policy;

d) The software token that can be used for subsequent identification and authentication with the TSF or other remote IT systems;

e) Active roles;

f) Active groups;

g) The effective and real user IDs;

h) The effective and real group IDs;

i) Rights profiles;

j) Privileges;

k) Authorizations]

FIA_USB.2.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [

a) Upon successful identification and authentication, the user identities shall be those specified via the user identifier attributes held by the TSF for the user;

b) Upon successful identification and authentication, the group identities shall be those specified via the group identifier attributes held by the TSF for the user.]

FIA_USB.2.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [

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]

FIA_USB.2.4: The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [

a) When executing a file which has the set UID[50] permission bit set, the effective user identity associated with the subject shall be changed to that of the owner of the file;

b) *When executing a file which has the set GID[51] permission bit set, the effective group identity associated with the subject shall be changed to that of the group attribute of the file*].

[50] UID – User Identifier
[51] GID – Group Identifier

Dependencies:	**FIA_ATD.1 User Attribute Definition**

Security Management

FMT_MSA.1 (LS)	**Management of security attributes**
Hierarchical to:	**No other components.**
FMT_MSA.1.1	The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy*] to restrict the ability to [modify] the **label-related object** security attributes to [*users that are authorized to assume identified roles*].
Dependencies:	**[FDP_ACC.1 Subset access control or** **FDP_IFC.1 Subset information flow control]** **FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MSA.1 (PSO)	**Management of object security attributes**
Hierarchical to:	**No other components.**
FMT_MSA.1.1	The TSF shall enforce the [*Persistent Storage Object Access Control Policy*] to restrict the ability to [modify**]** the security attributes [*of the objects covered by the SFP*] to [*the owner of the object and subjects with appropriate privileges*].
Dependencies:	**[FDP_ACC.1 Subset access control or** **FDP_IFC.1 Subset information flow control]** **FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MSA.1 (TSO)	**Management of object security attributes**
Hierarchical to:	**No other components.**
FMT_MSA.1.1	The TSF shall enforce the [*Transient Storage Object Access Control Policy*] to restrict the ability to [modify] the security attributes [*of the objects covered by the SFP*] to [*the owner of the object and subjects with appropriate privileges*].
Dependencies:	**[FDP_ACC.1 Subset access control or** **FDP_IFC.1 Subset information flow control]** **FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MSA.1 (VIRT-CACP)	**Management of security attributes**
Hierarchical to:	**No other components.**
FMT_MSA.1.1	The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Access Control Policy*] to restrict the ability to [change_default, query, modify] the security attributes [*of the subjects and objects covered by the SFP*] to **[***users that are authorized to assume identified roles*].
Dependencies:	**[FDP_ACC.1 Subset access control or** **FDP_IFC.1 Subset information flow control]** **FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MSA.1 (VIRT-CIFCP)	**Management of security attributes**
Hierarchical to:	**No other components.**
FMT_MSA.1.1	The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Information Flow Control Policy*] to restrict the ability to [change default, query, modify] the security attributes [*of the subjects and information covered by the SFP*] to [*users that are authorized to assume identified roles*].

Dependencies:	**[FDP_ACC.1 Subset access control or** **FDP_IFC.1 Subset information flow control]** **FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MSA.3 (LS) Static attribute initialisation

Hierarchical to:	**No other components.**
FMT_MSA.3.1	The TSF shall enforce the [*Multilevel Confidentiality Information Flow Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*users that are authorized to assume identified roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	**FMT_MSA.1 Management of security attributes** **FMT_SMR.1 Security roles**

FMT_MSA.3 (NI)	**Static attribute initialisation**
Hierarchical to:	**No other components.**
FMT_MSA.3.1	The TSF shall enforce the [*Network Information Flow Control Policy*] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*users that are authorized to assume identified roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	**FMT_MSA.1 Management of security attributes** **FMT_SMR.1 Security roles**

FMT_MSA.3 (PSO)	**Static attribute initialisation**
Hierarchical to:	**No other components.**
FMT_MSA.3.1	The TSF shall enforce the [*Persistent Storage Object Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*users that are authorized to assume identified roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	**FMT_MSA.1 Management of security attributes** **FMT_SMR.1 Security roles**

FMT_MSA.3 (TSO)	**Static attribute initialisation**
Hierarchical to:	**No other components.**
FMT_MSA.3.1	The TSF shall enforce the [*Transient Storage Object Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*users that are authorized to assume identified roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	**FMT_MSA.1 Management of security attributes** **FMT_SMR.1 Security roles**

FMT_MSA.3 (VIRT-CACP) Static attribute initialisation

Hierarchical to:	**No other components.**

FMT_MSA.3.1 The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users that are authorized to assume identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.3 (VIRT-CIFCP) Static attribute initialisation

Hierarchical to: **No other components.**

FMT_MSA.3.1 The TSF shall enforce the [~~*Compartment*~~ ***Zone*** *Information Flow Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users that are authorized to assume identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.4 (PSO) Security attribute value inheritance

Hierarchical to: **No other components.**

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes **for Persistent Storage Objects:** [*PSO objects inherit their security attributes from the object's ACL*].

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]

FMT_MTD.1 (AE) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify] the **[***set of audited events*] to [*users that are authorized to assume identified roles*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (AF) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [modify, add, delete] the **[***actions to be taken in case of audit storage failure*] to [*users that are authorized to assume identified roles*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (AM-AP) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [modify, *assign*] the [*security-relevant attributes*] to [*the authorised identified roles*] ***only after another user with the role [user assuming root role] has approved the action.***

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

Application Note: An attempt to assign or change any user security attribute by an authorized role is validated by the passmgmt service which is acting on behalf of the

root role to ensure that such modifications are consistent with rights that were granted to the authorized role.

FMT_MTD.1 (AM-MA) Management of TSF data

Hierarchical to:	**No other components.**
FMT_MTD.1.1	The TSF shall restrict the ability to [~~modify~~, *approve*]**,** the [*change or assignment operations of user security-relevant attributes performed by authorized identified roles that needs approval by users assuming root role*] to [*users that are authorized to assume identified roles*].
Dependencies:	**FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

Application Note: An attempt to assign or change any user security attribute by an authorized role is validated by the passmgmt service, which is acting on behalf of the root role to ensure that such modifications are consistent with rights that were granted to the authorized role.

FMT_MTD.1 (AM-MD) Management of TSF data

Hierarchical to:	**No other components.**
FMT_MTD.1.1	The TSF shall restrict the ability to **[**delegate, revoke delegation of, deny delegation of, deny sub-delegation of*, [sub-delegation of]*] the [*authorized identified roles*] to [*users granted that role*].
Dependencies:	**FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MTD.1 (AM-MR) Management of TSF data

Hierarchical to:	**No other components.**
FMT_MTD.1.1	The TSF shall restrict the ability to [modify**,** change default, delete, *create*] the [*assignment of roles to users down to the granularity of single users*] to [*users that are authorized to assume identified roles*]**.**
Dependencies:	**FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MTD.1 (AS) Management of TSF data

Hierarchical to:	**No other components.**
FMT_MTD.1.1	The TSF shall restrict the ability to [clear, create, delete] the **[***audit storage*] to [*users that are authorized to assume identified roles*].
Dependencies:	**FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MTD.1 (AT) Management of TSF data

Hierarchical to:	**No other components.**
FMT_MTD.1.1	The TSF shall restrict the ability to [modify, add, delete] the **[** *a) threshold of the audit trail when an action is performed;* *b) action when the threshold is reached*] to [*users that are authorized to assume identified roles*]**.**
Dependencies:	**FMT_SMF.1 Specification of management functions** **FMT_SMR.1 Security roles**

FMT_MTD.1 (EIA) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [initialize, modify, delete] the [*user security attributes used for the remote identification and authentication policy*] to [*users that are authorized to assume identified roles*]**.**

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (IAF) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [*re-enable*] the **[***authentication to the account subject to authentication failure***]** to [*users that are authorized to assume identified roles*]**.**

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (IAT) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [modify**]** the [*threshold for unsuccessful authentication attempts*] to [*users that are authorized to assume identified roles*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (IAU) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [initialize, modify, delete] the [*user security attributes*] to [*users that are authorized to assume identified roles*]**.**

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (NI) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete, change_default, and *no other operations*] the [*security attributes for the rules governing the*

a) identification of network data;
b) actions performed on the identified network data]

to [*users that are authorized to assume identified roles*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MTD.1 (VIRT-COMP) Management of TSF data

Hierarchical to: **No other components.**

FMT_MTD.1.1 The TSF shall restrict the ability to [initialize, modify, delete] the **[*~~compartment~~* *zone* *security attributes*] to [*users that are authorized to assume identified roles*]**.**

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_REV.1 (OBJ)	**Revocation**
Hierarchical to:	**No other components.**
FMT_REV.1.1	The TSF shall restrict the ability to revoke [*object security attributes defined by SFPs*] associated with the [*corresponding object*] under the control of the TSF to [*users that are authorized to assume identified roles*]**.**
FMT_REV.1.2	The TSF shall enforce the **following** rules:[*a) The access rights associated with an object shall be enforced when an access check is made;* *b) No other revocation rules.*]
Dependencies:	**FMT_SMR.1 Security roles**

FMT_REV.1 (USR)	**Revocation**
Hierarchical to:	**No other components.**
FMT_REV.1.1	The TSF shall restrict the ability to revoke [*user security attributes defined by the SFP*] associated with the [corresponding user] under the control of the TSF to [*users that are authorized to assume identified roles*].
FMT_REV.1.2	The TSF shall enforce the **following** rules: [*a) The enforcement of the revocation of security-relevant authorizations with the next user-subject binding process during the next authentication of the user;* *b) The immediate revocation of security-relevant authorizations*]
Dependencies:	**FMT_SMR.1 Security roles**

FMT_SMF.1	**Specification of Management Functions**
Hierarchical to:	**No other components.**
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [*a) Management of auditing;* *b) Management of cryptographic network protocols;* *c) Management of Persistent Storage Object Access Control Policy;* *d) Management of Transient Storage Object Access Control Policy;* *e) Management of Network Information Flow Control Policy;* *f) Management of Multilevel Confidentiality Information Flow Control Policy;* *g) Management of Zone Access Control Policy;* *h) Management of Zone Information flow Control Policy;* *i) Management of identification and authentication policy;* *j) Management of user security attributes;* *k) Management of TOE configuration data*]
Dependencies:	**No Dependencies**

FMT_SMR.1	**Security roles**
Hierarchical to:	**No other components.**
FMT_SMR.1.1	The TSF shall maintain the roles: [*a) User role with the following rights:* *i. Users are authorized to modify their own user password;*

ii. *Users are authorized to modify the access control permissions for the named objects they own;*
iii. *No additional rights*

b) *Users authorized by the RBAC policy to modify object security attributes*

c) *Users authorized by the Multilevel Confidentiality Information Flow Policy to modify object security attributes (When TX is enabled)*

d) *Users assuming administrative roles*]

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

Dependencies: **FIA_UID.1 Timing of identification**

Protection of the TSF

FPT_STM.1 **Reliable time stamps**

Hierarchical to: **No other components.**

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

Dependencies: **No dependencies**

FPT_TDC.1 **Inter-TSF basic TSF data consistency**

Hierarchical to: **No other components.**

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*access control and information flow control-related security attributes specified in Persistent Storage Access Control Policy and Network Information Flow Control Policy*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*the rules identified in FDP_ACF.1 (PSO), FDP_IFF.1 (NI), and subject authorizations*] when interpreting the TSF data from another trusted IT product.

Dependencies: **No dependencies**

FPT_TDC.1 (LS) **Inter-TSF basic TSF data consistency**

Hierarchical to: **No other components.**

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*label-related security attributes, no additional TSF data*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*comparison of label-related security attributes to determine if the security attributes are equal, greater or incomparable as defined in FDP_IFF.2 (LS)*] when interpreting the TSF data from another trusted IT product.

Dependencies: **No dependencies**

FPT_TDC.1 (VIRT) **Inter-TSF basic TSF data consistency**

Hierarchical to: **No other components.**

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*access control and information flow control related security attributes and no additional TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*zone access control permission settings as defined in FDP_ACF.1 (VIRT) and file-mac-profile as defined in FDP_IFF.1 (VIRT)*] when interpreting the TSF data from another trusted IT product.

Dependencies: **No dependencies**

TOE Access

FTA_SSL.1 **TSF-initiated session locking**

Hierarchical to: **No other components.**

FTA_SSL.1.1 The TSF shall lock an interactive session **to a human user maintained by the TSF** after [*an administrator-defined time interval of user inactivity*] by:

a) clearing or overwriting **TSF controlled** display devices, making the current contents unreadable;

b) disabling any activity of the user's **TSF controlled** data access/ **TSF controlled** display devices other than unlocking the session.

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

a) Successful re-authentication with the credentials of the user owning the session [*using one of the authentication methods out of the list of allowed methods specified in FIA_UAU.5*;

b) none]

Dependencies: **FIA_UAU.1 Timing of authentication**

FTA_SSL.2 **User-initiated locking**

Hierarchical to: **No other components.**

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

a) clearing or overwriting **TSF controlled** display devices, making the current contents unreadable;

b) disabling any activity of the user's **TSF controlled** data access/ **TSF controlled** display devices other than unlocking the session.

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

a) Successful re-authentication with the credentials of the user owning the session [*using one of the authentication methods out of the list of allowed methods specified in FIA_UAU.5*;

b) None]

Dependencies: **FIA_UAU.1 Timing of authentication**

Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: **No other components.**

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 **and** disclosure **using the following mechanisms.**

a) **Cryptographically-protected communication channel using [*the encryption protocols defined in FCS_COP.1(NET)*];**

b) **[*and no other mechanisms for trusted communication channels*].**

FTP_ITC.1.2 The TSF shall permit [the TSF or the trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*all security functions specified in the ST that interact with remote trusted IT systems and no other functions or conditions]*
Dependencies:	**No dependencies**

Security Assurance Requirements

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.3. Table 12 Assurance Requirements summarizes the requirements.

Table 12 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1* [52]Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.4 Production Support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM[53] Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.3 Systematic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: Basic Design
	ATE_FUN.1 Functional testing

[52] ASE_CCL.1 specified in CC Part 3 is refined. Refer to "Security Assurance Requirements Rationale" section in Chapter 8 for rationale.
[53] CM – Configuration Management

Assurance Requirements	
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused Vulnerability analysis

CHAPTER

7 TOE Summary Specification

TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 13 lists the security functions and their associated SFRs.

Table 13 Mapping of TOE Security Functionality Requirement

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible data loss
	FAU_STG.3(Remote)	Action in case of possible data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1(DSA)	Cryptographic key generation
	FCS_CKM.1(RSA)	Cryptographic key generation
	FCS_CKM.1(SYM)	Cryptographic key generation
	FCS_CKM.2(NET)	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(NET)	Cryptographic operation
	FCS_RNG.1	Random number generation
User Data Protection	FDP_ACC.1(PSO)	Subset access control

TOE Security Function	SFR ID	Description
	FDP_ACC.1(TSO)	Subset access control
	FDP_ACC.2(VIRT)	Complete access control
	FDP_ACF.1(PSO)	Security attribute based access control
	FDP_ACF.1(TSO)	Security attribute based access control
	FDP_ACF.1(VIRT)	Security attribute based access control
	FDP_ETC.2(LS)	Export of user data with security attributes
	FDP_ETC.2(VIRT)	Export of user data with security attributes
	FDP_IFC.2(LS)	Complete information flow control
	FDP_IFC.2(NI)	Complete information flow control
	FDP_IFC.2(VIRT)	Complete information flow control
	FDP_IFF.1(NI)	Simple security attributes
	FDP_IFF.1(VIRT)	Simple security attributes
	FDP_IFF.2(LS)	Hierarchical security attributes
	FDP_ITC.1(LS)	Import of user data without security attributes
	FDP_ITC.2	Import of user data with security attributes
	FDP_ITC.2(LS)	Import of user data with security attributes
	FDP_ITC.2(VIRT)	Import of user data with security attributes
	FDP_RIP.2	Full residual information protection
	FDP_RIP.3	Full residual information protection of resources
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(EIA)	User attribute definition
	FIA_ATD.1(HU)	User attribute definition
	FIA_ATD.1(LS)	User attribute definition
	FIA_ATD.1(TU)	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UAU.8(EIA)	Authentication policy decisions

TOE Security Function	SFR ID	Description
	FIA_UID.1	Timing of identification
	FIA_UID.2(VIRT)	User identification before any action
	FIA_UID.3(EIA)	Identification policy decisions
	FIA_USB.1(LS)	User-subject binding
	FIA_USB.2	Enhanced user-subject binding
Security Management	FMT_MSA.1(LS)	Management of security attributes
	FMT_MSA.1(PSO)	Management of object security attributes
	FMT_MSA.1(TSO)	Management of object security attributes
	FMT_MSA.1(VIRT-CACP)	Management of security attributes
	FMT_MSA.1(VIRT-CIFCP)	Management of security attributes
	FMT_MSA.3(LS)	Static attribute initialisation
	FMT_MSA.3(NI)	Static attribute initialisation
	FMT_MSA.3(PSO)	Static attribute initialisation
	FMT_MSA.3(TSO)	Static attribute initialisation
	FMT_MSA.3(VIRT-CACP)	Static attribute initialisation
	FMT_MSA.3(VIRT-CIFCP)	Static attribute initialisation
	FMT_MSA.4(PSO)	Security attribute value inheritance
	FMT_MTD.1(AE)	Management of TSF data
	FMT_MTD.1(AF)	Management of TSF data
	FMT_MTD.1(AM-AP)	Management of TSF data
	FMT_MTD.1(AM-MA)	Management of TSF data
	FMT_MTD.1(AM-MD)	Management of TSF data
	FMT_MTD.1(AM-MR)	Management of TSF data
	FMT_MTD.1(AS)	Management of TSF data
	FMT_MTD.1(AT)	Management of TSF data
	FMT_MTD.1(EIA)	Management of TSF data
	FMT_MTD.1(IAF)	Management of TSF data
	FMT_MTD.1(IAT)	Management of TSF data
	FMT_MTD.1(IAU)	Management of TSF data
	FMT_MTD.1(NI)	Management of TSF data
	FMT_MTD.1(VIRT-COMP)	Management of TSF data
	FMT_REV.1(OBJ)	Revocation
	FMT_REV.1(USR)	Revocation

TOE Security Function	SFR ID	Description
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_STM.1	Reliable time stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
	FPT_TDC.1(LS)	Inter-TSF basic TSF data consistency
	FPT_TDC.1(VIRT)	Inter-TSF basic TSF data consistency
	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.2	User-initiated locking
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel

Security Audit

The TOE can collect extensive auditing information about security-related actions taken or attempted by users, ensuring that users are accountable for their actions. Audit records are generated when specified auditable events occur. Events that generate audit records include the following:

- Startup and shutdown of the audit functions
- All auditable events for the basic and minimal level of audit as specified in Table 11
- All modifications to the set of events being audited
- All user authentication attempts
- All denied accesses to objects for which the access control policy defined in the OSPP base applies
- Explicit modifications of access rights to objects covered by the access control policies

Once the relevant event information has been captured, the information is formatted into an audit record. Contained in each audit record is the information that identifies the date and time of the event, type of event, subject identify (if applicable), and the outcome (success or failure) of the event. The audit record will also include the sensitivity labels of subjects, objects, or other information involved when TX is enabled. All audit records include a reliable timestamp.

For all user-related events, the audit records are associated with the identity of the user that caused the event. The TOE ensures that the audit trail storage shall be protected from unauthorized deletion, or prevent unauthorized modifications to the stored audit records. The TSF provides only the authorized roles or users with the ability to view audit records. The audit records are presented in a human-readable format. The authorized users map to the administrator configured roles with the corresponding rights profile, privileges, authorizations and supplementary rights profile (if applicable) assigned.

TSF allows for selection of events to be audited from the set of all auditable events based on the identity of users, subject identity, named object identity, the outcome of the audit event, subject and object sensitivity labels (when TX is enabled) and the audit class. Audit classes contain one or more audit events. Audit classes group together like

event types. Only administrative users may define classes of audit events. Only administrative users shall be able to define the default system audit-mask that defines which audit classes are recorded by default. 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 combined with the per-user audit-mask.

The system shall generate an alarm and notify an administrator, and writes a message to the machine console if the audit trail exceeds the defined audit threshold or "soft limit" as configured by the administrator, which may result in a loss of audit records. Soft limit is the minimum free space percentage available. The default is 1% free space percentage, but an authorized administrator can modify the default. In case of audit trail saturation the TSF shall drop the records that cannot be written and count the dropped records.

TOE can be configured to send the audit files to a remote repository for storage. A list of audit servers is specified in the configuration of audit_remote plugin. Audit_remote plugin is responsible for sending audit files to a remote server. The audit_remote plugin initiates a connection to first server in the list of audit servers specified. If the initiated connection is failed either because of timeout or network failure, the TSF attempts to connect to the next audit server from the list of audit servers specified after the administrator configured number of retries have been attempted on the previous server. The system shall generate an alarm and notify an administrator, and writes a message to the machine console indicating failure at every unsuccessful attempt to connect to the server.

TOE Security Functional Requirements Satisfied: FAU_GEN.1; FAU_GEN.2; FAU_SAR.1; FAU_SAR.2; FAU_SEL.1; FAU_STG.1; FAU_STG.3; FAU_STG.3 (Remote), FAU_STG.4.

Cryptographic Support

All crypto services in the evaluated configuration are provided by FIPS-validated cryptographic modules. The FIPS 140-2 certificates of the crypto modules used by TOE are #1051, #2061 and #2077, and have been issued by the CMVP.

The TOE provides cryptographic functionality for authentication, data protection, and communications security purposes. This functionality includes symmetric, asymmetric, hashing, random number generation, and message authentication code algorithms. In order to provide this functionality to various applications and operating system components in an elegant, optimized fashion, Oracle has included within the TOE the Solaris Cryptographic Framework. The Solaris Cryptographic Framework itself does not contain cryptographic algorithms, rather it provides a unified API for applications executing at both the user-level and kernel-level to access cryptographic algorithms from multiple provider "plug-ins". The Solaris Cryptographic Framework has two parts, the user-level cryptographic framework and the kernel-level cryptographic framework.

The Oracle Solaris Cryptographic Framework's architecture is depicted in Figure 3 below. Acronyms referenced in this diagram that have not previously been defined are:

- Data Encryption Standard (DES),
- Message Digest 5 Algorithm (MD5), and
- Triple Data Encryption Standard (3DES).

Note: /dev/crypto is not part of the evaluated configuration.

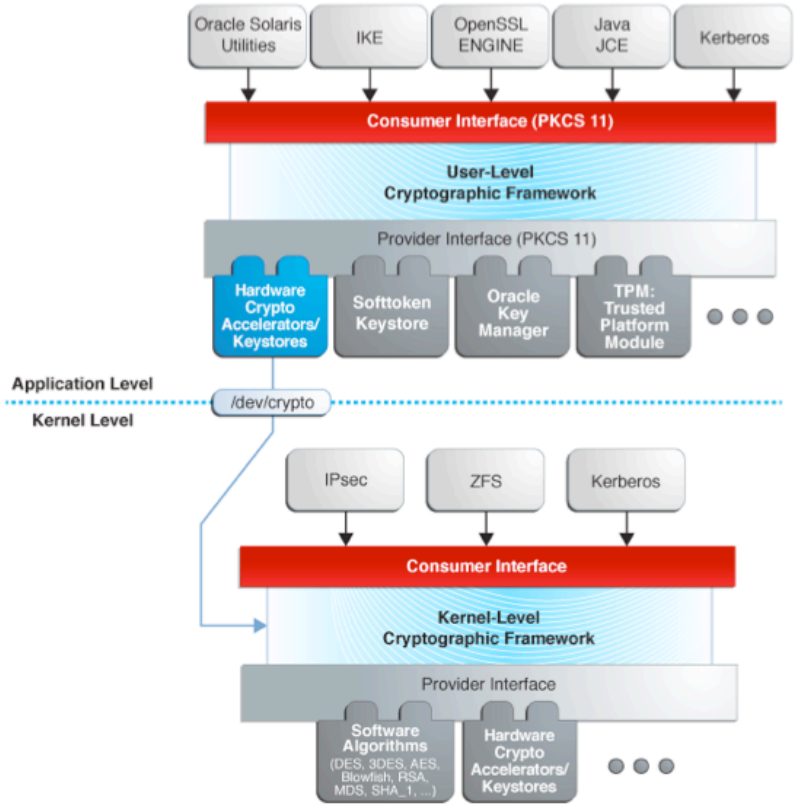


Figure 3 Oracle Solaris Cryptographic Framework

The user-level cryptographic framework and kernel-level cryptographic framework are discussed in more detail in the chapters below.

User-Level Cryptographic Framework

All user-level software within the TOE requiring cryptographic services makes use of the user-level cryptographic framework's consumer API based on RSA PKCS #11 v2.11. The only exception is SSH, which uses a private interface to a FIPS validated OpenSSL library. Depicted above the API is the actual user-level cryptographic framework, which is mostly logic intended to glue the many cryptographic providers together and make them appear as a single aggregate provider. These cryptographic providers contain the actual implementations of cryptographic algorithms. The PKCS #11provider interface exposes a list of cryptographic "slots" that enable the application to select the provider that best suits the application's particular needs. In the evaluated TOE, all providers must undergo digital signature verification in order to be aggregated by the framework. The framework uses the Module Verification Daemon (not depicted) to verify that the provider is authorized for use, and to determine if there are usage restrictions on the provider. The signature is associated with an RSA key included in a certificate issued by Oracle.

Kernel-Level Cryptographic Framework

The kernel-level cryptographic framework provides cryptographic services to kernel modules, devices drivers, and the user-level cryptographic framework via the

cryptographic providers with a proprietary API. Like the user-level cryptographic framework, the kernel-level cryptographic framework does not itself contain cryptographic algorithms; rather it leverages plug-ins using a proprietary API that is more applicable for kernel modules and device drivers from Oracle and from third parties. In addition to this public API, the kernel-level cryptographic framework exposes two private device drivers, /dev/random and /dev/cryptoadm. User-level cryptographic framework uses /dev/random (via a provider) to receive entropy from the kernel-level cryptographic framework. The module verification daemon and the cryptoadm(1M) command use /dev/cryptoadm to communicate with the kernel-level cryptographic framework.

Additionally, kernel-level cryptographic framework provides scheduling and load balancing for cryptographic operations for the kernel consumer, as well as offers an asynchronous mode for the consumer interface routines.

Cryptography Consumers

As mentioned above, the Solaris Cryptographic Framework provides cryptographic functionality for applications, kernel modules, and device drivers within the TOE to use for authentication, data protection, and securing communications.

Authentication: The TOE utilizes cryptography for various purposes related to authentication. By default, the TOE hashes passwords for user accounts using the SHA-256 or SHA-512 algorithms. For users connecting to the TOE via Solaris SSH, the TOE allows for them to authenticate with a password, which is hashed, through the GSSAPI, which leverages Kerberos, or with digital certificates in public key authentication. Additionally, IPsec peers can be authenticated using IKE and pre-shared keys for authentication.

The Kerberos V5 network authentication protocol provides an integrated client/server architecture that offers strong user authentication, as well as data integrity and privacy, for providing secure transactions over networks. Kerberos can also verify the validity of data being passed back and forth (integrity) and encrypt it during transmission (privacy/confidentiality). NFS service can uses Kerberos V5 for authentication.

In addition to user authentication, the TOE implements SASL to provide authentication and optional security services to network protocols. Security services are provided by SASL plug-ins, which are included in the evaluated configuration, and the GSSAPI, which relies on an existing Kerberos infrastructure.

Data Protection: The TOE can be configured to protect stored user and system data with encryption. The TOE provides an end-user interface as part of the SSH implementation. End users can directly interact with the user-level cryptographic framework with user-level commands. These commands include:

- Digest – Computes a message digest for one or more files or for stdin. A digest is useful for verifying the integrity of a file. SHA1, SHA256, SHA384 and SHA512 are the digest functions used.
- MAC – Computes a message authentication code for one or more files or for stdin. A message authentication code associates data with an authenticated message. A message authentication code enables a receiver to verify that the message came from the sender and that the message has not been tampered with. The sha1_hmac, sha256_hmac, sha384_hmac and sha512_hmac mechanisms can compute a message authentication code.
- Encrypt – Encrypts files or stdin with a symmetric cipher. The encrypt–l command lists the algorithms that are available. Mechanisms that are listed under a user-level library are available to the encrypt command. The framework provides AES, and TDES mechanisms for user encryption.

- Decrypt – Decrypts files or stdin that were encrypted with the encrypt command. The decrypt command uses the identical key and mechanism that were used to encrypt the original file.

Communications Security: In its evaluated configuration, Solaris 11 supports trusted communication channels for TCP and IP layer connections between different physical TOEs through different protocols/services. These protocols include SASL, Kerberos, and IPsec with IKE and pre-shared keys as provided to applications via the User-level Cryptographic Framework or Kernel Cryptographic Framework. Additionally, SSH provides trusted communications via an OpenSSL implementation. Each of these protocols can be configured to use one of many provided cipher suites.

TOE Security Functional Requirements Satisfied: FCS_CKM.1 (DSA); FCS_CKM.1 (RSA); FCS_CKM.1 (SYM); FCS_CKM.2 (NET); FCS_CKM.4; FCS_COP.1 (NET); FCS_RNG.1.

User Data Protection

The User Data Protection family defines the Persistent Storage Object Access Control Policy, Transient Storage Object Access Control Policy, Network Information Flow Control Policy, Multilevel Confidentiality Information Flow Control Policy, Zone Access Control Policy and Zone Information Flow Control Policy, each of which are discussed below.

Persistent Storage Object Access Control Policy

Persistent storage objects are objects that hold user and/or TSF data that retain the stored data during initialization, re-initialization and power-cycling of the TOE. The TOE enforces PSO Access Control Policy on all operations among subjects and objects covered by the PSO Access Control Policy. The allowed operations on the objects by the PSO Access Control Policy are create, delete, enable, disable, modify, read, write and execute. The persistent storage objects are of the following types: data sets, terminals, devices, volumes, consoles, operator commands, programs, file system objects (such as regular files, directories, symbolic links, character special files).

The PSO Access Control Policy uses UNIX permissions and ACLs to determine access to data on the TOE.

UNIX file permissions assign ownership to three classes of users:

- User: The file or directory owner, which is usually the user who created the file. The owner of a file can decide who has the right to read the file, to write to the file, or, if the file is a command, to execute the file.
- Group: Members of a group of users.
- Others: All other users who are not the file owner and are not members of the group.

Within the TOE, PSO is applied in two different ways depending on the type of object. This security target therefore defines two object types:

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

The owner of the object can assign or modify permissions associated with that object. Note, however, that users assuming root role will have access to all objects on the system. Access permission to the objects by users not already possessing access permission will only be assigned by an authority responsible and authorized to grant

access. The TOE allows user or group IDs to be specified as effective or real. The real UID/GID is the UID/GID who owns or starts the process. The effective UID/GID is the UID/GID the process runs as. The PSO uses 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.

The permissions that are available for each class of user for a file or directory are: read, write, execute and denied. These permissions apply to all regular files, and to special files such as devices. For a symbolic link, the permissions that apply are the permissions of the file that the link points to. The files in a directory and its subdirectories can be protected by setting restrictive file permissions on that directory.

Three special types of permissions are available for executable files and public directories: setuid, setgid, and sticky bit[54]. When executing a file which has the setuid permission bit set, the effective user identity associated with the subject shall be changed to that of the owner of the file. When executing a file which has the setgid permission bit set, the effective group identity associated with the subject shall be changed to that of the group attribute of the file. The effective user identity associated with a subject can be changed to another user's identity provided that the subject possessed an override privilege or successful authentication as the new user identity has been achieved.

If a directory is writable and has the sticky bit set, files within that directory can be removed or renamed only if one or more of the following is true:

- The user owns the file
- The user owns the directory
- The file is writable by the user

If a regular file is not executable and has sticky bit set, the file is assumed to be a swap file. In this case, the system's page cache will not be used to hold the file's data. If the sticky bit is set on any other file, the results are unspecified.

The PSO mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. The PSO will be capable of including or excluding access down to the level of a single user.

Transient Storage Object Access Control Policy

Transient storage objects are objects that hold user and/or TSF data that do not retain the stored data during initialization, re-initialization and power-cycling of the TOE. Transient storage objects are volatile storage objects, and can be re-used when re-allocation is performed.

The TOE enforces the TSO Access Control Policy on all operations among subjects and objects covered by the TSO Access Control Policy. The transient storage objects for the TOE are the objects belonging to the System V IPC mechanisms, POSIX IPC mechanisms, signals, named pipes and sockets. System V IPC mechanisms are shared memory, message queues, semaphores. The shared memory mechanism allows processes to attach (map) system memory spaces to their virtual address spaces and this mapped memory with other processes. The messages queue mechanism allows co-operating processes to send and to receive formatted data between themselves. The semaphore mechanism allows processes to synchronize their execution using mutually exclusive access to critical chapters of code or to critical or limited resources. POSIX IPC is a variation of System V IPC. Signals are a special type of IPC mechanism. Signals are asynchronous notifications sent to a process or to a specific thread within the same process in order to notify it of an event that occurred. Named pipes allow you to

[54] Sticky bit – Sticky bit is a permission bit that protects the files within a directory

connect the output of one process to the input of another. Sockets are data communication end points for exchanging data between processes executing within the same host OS.

Access rights to TSO are granted based on the user identity and group memberships associated with a subject. The TSO SFP uses UNIX permission bits to regulate the access to the TSO objects. Operations on a TSO are granted to a process if the effective user ID or group ID of the process matches the owner's user ID or group ID, or creator's user ID or group ID in the data structure associated with the system V IPC object, and the appropriate bit of the "user" portion, or "group" portion of the data structure is set respectively. Or the access is granted to a process if the "other" portion of the data structure is set. However if a subject has an effective override privilege, the TSF shall authorize access of the subject to any given object.

The TOE grants access to objects in the kernel by controlling the access to the interfaces that are provided by kernel. Kernel provides a standard interface called "System V IPC" interface to access the TSO.

Network Information Flow Control Policy

The Network Information Flow Control Policy defines the rules to identify the network data and the operation to be performed on the network data. The TOE allows filtering of network data using Network Information Flow Control Policy. The TOE supports stateful packet filtering. The filtering functionality is limited to static filter rules for the protocols stated below.

The TOE enforces Network Information Flow Control Policy on all unauthenticated external IT entities that send and receive information mediated by the TOE. The TOE enforces Network Information Flow Control Policy on all the network data routed through the TOE and all operations that cause the information to flow to and from the subjects covered under SFP.

The TOE enforces the Network Information Flow Control Policy based on the following security attributes:

- The logical or physical network interface through which the network data entered the TOE
- Source and destination IP address
- Source and destination TCP port number
- Source and destination UDP port number
- Network protocol (IP, IPv4, IPv6, TCP, UDP, ICMP, ARP, SCTP, IPsec)
- TCP header flags of SYN, ACK
- VLAN tag

The TOE performs the network information flow control based on initially identifying network data and subsequently performing actions on the network data. The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation for matching based on the information security attributes and the state of the TCP connection. The TOE shall either discard the identified network data without any further processing or allow it unaltered as per the routing information maintained by the TOE.

The TSF provides permissive default values for security attributes that are used to enforce Network Information Flow Control Policy. The TSF restricts the ability of authorized users to query, modify, delete, or change_default settings of the security attributes associated with the rules governing the identification of network data, and actions to be performed on the identified network data.

Multilevel Confidentiality Information Flow Control Policy

Multilevel Confidentiality Information Flow Control Policy is a system-enforced MAC mechanism when TXs are enabled. It is an access control mechanism based on label relationships. By default, TXs provide single-label services, however multilabel (multilevel) services can be configured. TXs software protects information and other resources through both DAC and MAC. DAC is the traditional UNIX permission bits and access control lists that are set at the discretion of the owner. MAC is a mechanism that the system enforces automatically. MAC controls all transactions by checking the labels of processes and data in the transaction. With Trusted Extensions, both MAC and DAC (if configured) coexist, and DAC checks and MAC checks must pass before access is allowed to an object.

Trusted Extensions define a label called a sensitivity label (label). Sensitivity labels are assigned to subjects, and objects such as:

- Data sets
- Terminals
- Volumes
- Consoles
- Operator commands
- Programs,
- Devices
    - Allocatable devices such as tape drives, diskette drives, CD-ROM and DVD devices, and audio devices; and
    - Not allocatable devices such as printers, workstations and serial lines when they are used as login device
- File system objects (such as regular files, directories, symbolic links, character special files).
- Network interfaces
- Windows

Each sensitivity label has two components: classification (level) and compartment (category). Classification indicates sensitivity label's a relative level of protection. Compartments are optional, and can be used to represent different kinds of groupings, such as workgroups, departments, divisions or geographical areas. A sensitivity label's classification field can contain up to 255 values and its compartment field can contain up to 256 bits of information. The user attributes associated with sensitivity labels are clearance and min_label. Clearances are the least upper bounds for sensitivity labels. The user's clearance determine the highest level at which a user is permitted to operate. Min_label contains the minimum label at which the user can log in. Objects can also be specified with a label range. The ADMIN_HIGH label and the ADMIN_LOW label are administrative labels, and define the upper bound and lower bound of all labels on a system.

Labeled TOE objects and subjects are vital to the secure import and export of user data. Labels provide a set of rules that are enforced by the TOE to protect information that is being processed on the TOE. Objects and subjects are given labels in which their relationship determines the types of access that are given to each.

Information flow is allowed between a subject and object based on their label information. Relationship between the labels can be classified as dominate, equal and disjoint. One entity's label is said to dominate another label if the classification component of the first entity's label is equal to or higher than the second entity's label, and the set of compartments in the first entity includes all of the second entity's compartments. Two labels are said to be equal if they have same classification and same set of compartments. Two labels are said to disjoint if neither label dominates the other. The authorized identified roles with appropriate authorizations such as

"solaris.label.win.downgrade", "solaris.label.win.upgrade", or "solaris.label.win.noview" can move information from a higher-level file and place that information in a lower-level file; from a lower-level file and place that information in a higher-level file; or move information between files without viewing the information that is being moved respectively.

The TOE administrator is the person who plans, defines, and implements the values and bits that define the internal representation of the labels. The default policy is view and modify access of equal labels. This can be configured to be view access of dominated labels and modify access of equal labels. When unlabeled data enters the TOE, it is automatically labeled based on the policy rules that the TOE administration has previously established.

All network ports are single-label by default and can only be used between peers with matching labels.

The TSF restricts the ability to modify the label-related security attributes to the authorized users only. The TSF provides restrictive default values for security attributes that are used to enforce Mandatory Access Control Policy. It is up to the authorized identified roles to specify the alternate initial values for security attributes to override the default values.

Zone Access Control Policy

Zones are virtualized operating system environments created within a single instance of the TOE. Zones provide a virtualized, isolated, and secure environment for operating system services, processes, and individual applications. The Zone Access Control Policy is enforced on TOE subjects and objects as identified in the Persistent Storage Object Access Control Policy, and Transient Storage Object Access Control Policy.

Global zone is the default zone for the system, and is the zone used for system-wide administrative control. There can only be a single global zone; however, Oracle Solaris 11 supports creation of multiple non-global zones. When a non-global zone is created, an application execution environment is produced, in which processes are isolated from the rest of the system. This isolation prevents processes that are running in one zone from monitoring or accessing processes that are running in another zone (See Zone Information Flow Control Policy). Processes within a zone are allowed to manipulate, monitor, and directly communicate with other processes in the same zone. Processes that are assigned to different zones are only able to communicate through network APIs.

Zone Access Control Policy is based on the following security attributes, zone ID, IP type, zone privileges, data link(s), process ID, file system zone mount point(s). The Zone Access Control Policy enforces access to a zone by an object based on the mode of access that is set up for the zone and which access control permissions are set for that object. The TSF shall authorize access of the subject to any object in any given zone if the subject has override privileges. Only authorized roles, or users have the ability to query, modify, or change the restrictive default values of the security attributes.

The TSF enforces Zone Access Control Policy and Zone Information Flow Control Policy on all user data that is imported, and exported to and from zones. The TSF ensures that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data. The TSF ensures that the security attributes of the imported user data are interpreted correctly as intended by the source of the user data during importation.

Zone Information Flow Control Policy

The Zone Information Flow Control Policy is enforced on TOE subjects, external entities as well as on TOE information. The information could be user data belonging to subjects inside and outside of the zones. The Zone Information Flow Control Policy ensures the secure import and export of zone user information. As discussed in the Zone Access Control Policy, when a zone is created, an application execution environment is produced, in which subjects are isolated from the rest of the system. This isolation prevents subjects that are running in one zone from monitoring or accessing processes that are running in another zone. Therefore, information flow between subjects and objects of the TOE may only flow within the same zone. One exception to this is when networking API calls are used.

The Zone Information Flow Control Policy is based on zone subject security attributes such as zone IP address and the root sub-directory file system. The Zones SFP is also based on zone information security attributes for user and TSF data such as ACL and permission bits, and the file-mac-profile property.

A zone's file-mac-profile property is its defining property which controls write access and information flow to the zone's root sub-directory file system. The implementation is held in the zone brand configuration files in the global zone, which is unreachable or uneditable from inside a non-global zone. The file-mac-profile can be set to one of 4 values: none, strict, fixed configuration and flexible configuration. The policy cannot be changed from inside a non-global zone; only the global zone is allowed to set the policy before any processes in the non-global zone are running. Setting this value to:

- None allows read/write access to zone
- Strict allows no exceptions to the read-only policy
- Fixed-configuration allows the zone to write to files in and below /var, except directories containing configuration files:
  - /var/ld
  - /var/lib/postrun
  - /var/pkg
  - /var/spool/cron
  - /var/spool/postrun
  - /var/svc/manifest
  - /var/svc/profiles
- Flexible-configuration is equal to fixed-configuration but allows writing to files in /etc in addition.

Once a zone has been fully configured, the ability to query, modify or change the restrictive default values (IP network configuration and file-mac-profile) of the zone is restricted to the authorized roles, or users.

Full Residual Information Protection

The TSF offers full residual information protection of resources. It ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects, subjects or users.

TOE Security Functional Requirements Satisfied: FDP_ACC.1 (PSO); FDP_ACC.1 (TSO); FDP_ACC.2 (VIRT); FDP_ACF.1 (PSO); FDP_ACF.1 (TSO); FDP_ACF.1 (VIRT); FDP_ETC.2 (LS); FDP_ETC.2 (VIRT); FDP_IFC.2 (LS); FDP_IFC.2 (NI); FDP_IFC.2 (VIRT); FDP_IFF.1 (NI); FDP_IFF.1 (VIRT); FDP_IFF.2 (LS); FDP_ITC.1 (LS); FDP_ITC.2; FDP_ITC.2 (LS); FDP_ITC.2 (VIRT); FDP_RIP.2; FDP_RIP.3.

Identification and Authentication

TOE users are external entities that interact with the TOE. Such external entities include human users and technical users such as other IT systems. The TOE identification and authentication functionality enforces TOE users to successfully identify and authenticate to the TOE to access its functionality. If zones are configured, the TSF shall require each zone user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

The TOE maintains the following security attributes belonging to individual human users, or technical users:

- User ID
- Group membership
- User password
- Software token verification data
- Security roles
- Rights profiles
- Privileges
- Authorizations
- Kerberos ticket lifespan
- X.509 v3 certificates
- Indication off the authentication algorithm used by the IPsec, Kerberos, SASL, SSH
- Sensitivity label (when TX is enabled)
- Logical or physical network interface through which the network data entered the TOE
- Identity of the logical or physical external interface through which the user connected to the TOE
- Source and destination IP addresses, and
- Source and destination ports.

The TOE provides protected authentication feedback; on entry passwords shall not be displayed in cleartext and are obscured. The TOE will lock out a user account if the user fails to enter the proper credentials after an administrator-configured number of unsuccessful authentication attempts have been met or surpassed.

The TOE enforces minimum password strength requirements. The password quality metric must meet the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20.

The TOE allows the user to select language, desktop or console or remote host for login, select fail safe login and login help function on behalf of the user to be performed before the user is authenticated, and "Universal access preferences" [55]before being identified. The TSF allows the information flow covered by the Network Information Flow Control Policy on behalf of the user to be performed before the user is authenticated. For all

[55] Universal access preferences include
- Use screen reader
- Use screen magnifier
- Enhance contrast in colors
- Make text larger and easier to read
- Press keyboard shortcuts one key at a time (Sticky Keys)
- Ignore duplicate keypresses (Bounce Keys)
- Press and hold keys to accept them (Slow Keys)

other TSF-mediated actions TOE requires users to be successfully identified and authenticated.

The TOE provides multiple authentication mechanisms such as authentication based on username, and password; authentication based on software token verification data; authentication based on digital certificates, and Kerberos tickets; and public key authentication to support user authentication. The TOE supports these multiple authentication mechanisms via a pluggable framework (PAM) such as local files username and password, and Kerberos (or combination of those), giving TOE users a convenient way to identify and authenticate themselves to the TOE. The other authentication mechanisms that TOE support include SASL, a framework that provides authentication and security services to network protocols; and SSH, a secure remote login and transfer protocol. In SSH, authentication is provided by the use of public keys, and user credentials.

The TOE allows users to connect remotely and transmit user credentials from client machines/remote IT entities to the TOE. The TOE uses the security attributes such as UNIX user identifier and password, or Kerberos user identifier and password (or combination of those) for identifying and authenticating users connecting remotely. The TOE shall communicate the identification and authentication policy decision back to client machines/remote IT entities. The TOE serves as an authentication server and provides authentication service to remote trusted IT entities through the use of the Kerberos service.

When TX is enabled, the TOE also maintains the information about user attributes associated with sensitivity labels such as clearance and min_label. Clearances contains the maximum label at which an user can operate, they are the least upper bounds for sensitivity labels. Min_label contains the miminum label at which an user can log in. The sensitivity label associated with a subject shall be within the clearance range of the subject.

For subjects acting on behalf of the user, the TSF shall provide the user-subject binding. In the process of user-subject binding, the TSF shall be to associate the user security attributes such as active roles, and groups; effective and real user IDs and group IDs; rights profiles; privileges; authorizations; security attributes used to enforce Persistent Storage Object Access Control Policy, and Transient Storage Object Access Control Policy; or UID associated with auditable events to a subject acting on behalf of a user. In the evaluated configuration this information can be stored locally in database files or in an LDAP repository, which resides in TOE environment.

Upon successful identification and authentication, the subjects acting on behalf of the users assume the UID, or GID attributes held by the TSF for that user. The effective UID associated with a subject can be changed to another user's identity if the effective user carried overrides privileges or when a new user has been successfully authenticated. In the instances, when the executable files have set UID permission bit or set GID permission bit set, the effective UID or GID associated with the subject shall be changed to the owner of the file or the group attribute of the file.

TOE Security Functional Requirements Satisfied: FIA_AFL.1; FIA_ATD.1(EIA) FIA_ATD.1(HU); FIA_ATD.1(LS); FIA_ATD.1(TU); FIA_SOS.1; FIA_UAU.1; FIA_UAU.5; FIA_UAU.7; FIA_UAU.8(EIA); FIA_UID.1; FIA_UID.2(VIRT); FIA_UID.3(EIA); FIA_USB.1(LS); FIA_USB.2.

Security Management

Security management specifies how the TOE manages several aspects of the TSF including TSF data and security functions. The TOE provides administrators with the ability to manage security attributes for the TOE.

The TOE allows authorized identified users, or roles to manage the security attributes associated with Persistent Storage Object Access Control Policy, Transient Storage Object Access Control Policy, Multilevel Confidentiality Information Flow Control Policy, Zone Access Control Policy, Zone Information Flow Control Policy, and Network Information Flow Control Policy.

The TOE implements RBAC functionality to selectively grant administrative rights to users or roles as needed. It allows controls on user access to tasks that would otherwise be denied. It is the policy of authorizations to permit certain userlevel operations that would otherwise be denied by the userland portion of the SFP, and the policy of privileges to permit certain kernel level operations that would otherwise be denied by the kernel portion of the SFP. When TX is enabled, additional privileges are interpreted by user land components of the desktop window system and the label service.

Administrative rights can be distributed among several administrators as needed. The TOE utilizes a Service Management Facility (SMF) services to add, remove, configure, and manage services. SMF relies on RBAC to control access to service management functions on the TOE.

All TOE management functions are restricted to the TOE authorized identified users, or roles. All object security attributes contain restrictive default values. It is up to the authorized identified users, or roles to modify the default values for each of the rights profiles. Each user of the TOE will be assigned a role with one or more rights profiles, which will determine their level of access within the TOE.

Role-based Access Control (RBAC) Policy

Oracle Solaris RBAC is a more secure alternative to a traditional superuser model. RBAC is a security feature for controlling user access to tasks that would normally be restricted to the root role. By applying security attributes to users and processes, RBAC can divide up superuser capabilities among several administrators.

The traditional UNIX root account is a role by default in the TOE. Authorized users can assume the root role rather than directly logging into a root user account. During installation, the first user account is assigned the root role.

User rights management is implemented through RBAC. RBAC components include roles, and rights profiles. RBAC collects superuser capabilities into rights profiles. These rights profiles are assigned to special user accounts that are called roles, and roles are assigned to users. Rights profiles can contain authorizations, privileges, privileged commands, and other supplementary rights profiles.

A role is a special type of user account from which you can run privileged applications. Roles are created in the same general manner as user accounts. Rights profiles and authorizations give the role administrative capabilities. Roles cannot inherit capabilities from other roles or other users.

In addition to the default progenitor root role delivered by the TOE, configuration of some additional roles are recommended:

- A System Administrator role to perform non-security relevant administration, which is granted the System Administration, rights profile.
- An Operator role to perform simple administration, which is granted the Operator, rights profile.
- A User Management role to perform non-security relevant user and role management, which is granted the User Management, rights profile.

- A User Security role to perform the remaining user and role management tasks, which is granted the User Security, rights profile.

In addition, it is also recommended to configure one or more security roles for network security administration.

Rights profiles are a collection of administrative capabilities that can be assigned to a role or to a user. The available rights in Solaris OS are:

- System Administrator rights profile: Provides a profile that can do most tasks that are not connected with security.
- Operator rights profile: Provides limited capabilities to manage files and offline media.
- Printer Management rights profile: Provides a limited number of commands and authorizations to handle printing.
- Basic Solaris User rights profile: Enables users to use the system within the bounds of security policy. This profile is listed by default in the policy.conf file.
- Console User rights profile: Is granted by default to the user who logs in on the console. It provides for those user authorizations, commands and sub-profiles necessary for managing various functions that are normally provided for a user to control their personal system.
- All rights profile: For roles, provides access to commands that do not have security attributes.
- Stop rights profile: Is a special rights profile that stops the evaluation of further profiles. The Stop rights profile prevents the evaluation of the AUTHS_GRANTED, PROFS_GRANTED, and CONSOLE_USER variables in the policy.conf file.
- Additional rights profiles can be created as needed by users assuming the root role.

Authorization is a permission that enables a user or role to perform a class of actions that requires additional rights. Authorizations enforce policy at the user application level. Authorizations can be assigned directly to a role or a user.

Process rights management is implemented through privileges. A privilege is a discrete right that can be granted to a command, a user, a role, or a system. It is a right that a subject requires to perform an operation. Privileges enable a process to succeed. Privileges enforce security policy in the kernel. Without the proper privilege, a subject can be prevented from performing privileged operations by the kernel.

Privileges work with RBAC to provide a more secure administration alternative than administration of a system by a superuser. RBAC uses the security principle of least privilege. Least privilege means that a subject has precisely the amount of privilege that is necessary to perform a job. Privileged commands are commands that execute with security attributes.

The Supplementary profiles reflect the role's primary tasks, and allow the role privileges to be defined in a more granular fashion. For example, the Operator rights profile contains two supplementary profiles such as Printer management and Media backup.

TOE Security Functional Requirements Satisfied: FMT_MSA.1 (LS); FMT_MSA.1 (PSO); FMT_MSA.1 (TSO); FMT_MSA.1 (VIRT-CACP); FMT_MSA.1 (VIRT-CIFCP); FMT_MSA.3 (LS); FMT_MSA.3 (NI); FMT_MSA.3 (PSO); FMT_MSA.3 (TSO); FMT_MSA.3 (VIRT-CACP); FMT_MSA.3 (VIRT-CIFCP); FMT_MSA.4 (PSO); FMT_MTD.1 (AE); FMT_MTD.1 (AF); FMT_MTD.1 (AM-AP); FMT_MTD.1 (AM-MA); FMT_MTD.1 (AM-MD); FMT_MTD.1 (AM-MR); FMT_MTD.1 (AS); FMT_MTD.1 (AT); FMT_MTD.1 (EIA); FMT_MTD.1 (IAF); FMT_MTD.1 (IAT); FMT_MTD.1 (IAU); FMT_MTD.1 (NI); FMT_MTD.1 (VIRT-COMP); FMT_REV.1 (OBJ); FMT_REV.1 (USR); FMT_SMF.1; FMT_SMR.1.

Protection of the TSF

The TOE provides reliable time stamps, which can be changed or set manually by the administrator. The time can be synchronized to Coordinated Universal Time manually through the configuration settings. The TOE also provides for configuring NTP server, which allows setting and maintaining the system time. Administrators are assumed to be trusted and competent, and may change the system time whenever necessary. The reliable time stamps are used in audit record generation.

The TSF ensures that access control and information flow control-related security attributes specified in Persistent Storage Object Access Control Policy, Transient Storage Object Access Control Policy and Network Information Flow Control Policy are consistently interpreted when shared between the TSF and other trusted IT products. The TSF uses the security based access control rules instructed by the Persistent Storage Object Access Control Policy, Transient Storage Object Access Control Policy and Network Information Flow Control Policy when interpreting the TSF data from another trusted product.

When TXs are enabled, the TSF provides the capability to consistently interpret label-related security attributes when shared between the TOE and another trusted IT product. The TSF shall compare the label-related security attributes such as sensitivity labels to determine if the security attributes are equal, greater or incomparable when interpreting the TSF data from another trusted IT product.

The TSF provides the capability to consistently interpret the access control and information flow control related security attributes associated with zones when shared between the TSF and another trusted IT product. The TSF shall use the zone access control permission settings and zone file-mac-profile when interpreting the TSF data from another trusted IT product.

TOE Security Functional Requirements Satisfied: FPT_STM.1; FPT_TDC.1; FPT_TDC.1 (LS); FPT_TDC.1 (VIRT).

TOE Access

The TOE mitigates unauthorized user access by automatically locking a user session after an administrator predefined time interval of inactivity. Once the session is locked, the TSF will clear or overwrite TSF controlled display devices, ensuring the current contents are unreadable. Locking the session will disable any activity of the user's TSF controlled data access and TSF controlled display devices other than unlocking the session.

The TOE allows user-initiated locking of the user's own interactive session maintained by the TSF by clearing or overwriting TSF controlled display devices, ensuring the current contents are unreadable. User-initiated locking session will disable any activity of the user's TSF controlled data access and TSF controlled display devices other than unlocking the session.

In order for an authorized user to regain access of a locked out session, the user must successfully re-authenticate with the credentials of the user owning the locked out session by using one of the allowed authentication methods.

TOE Security Functional Requirements Satisfied: FTA_SSL.1; FTA_SSL.2

Trusted Path/Channels

The TSF provides cryptographically protected communication channels between itself and other IT trusted products. In its evaluated configuration, the TOE supports trusted communication channels for TCP and IP layer connections. The TOE supports SSH, IPsec, SASL and Kerberos protocols to cryptographically secure the communications between itself and other trusted IT products that is logically distinct from other communication channels. In all those cases, the TSF ensures that the data exchanged between the TOE and the remote trusted IT system is sufficiently protected against modification and disclosure. It also provides assured identification of the end points involved. Either the TOE or the other trusted IT product can initiate communication via the trusted channels. Secure channel between TOE and LDAP server can be established using SASL/GSSAPI or IPsec protocols.

TOE Security Functional Requirements Satisfied: FTP_ITC.1

CHAPTER

8 Rationale

Conformance Claims Rationale

This Security Target extends to Part 2 and conforms to Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3. This ST conforms to the PP as specified in Table 3.

Variance Between the PP and this ST

- FDP_IFF.2 (LS) TX supports 255 site-definable hierarchical levels called classifications and 2^{256} site-definable non-hierarchical category bits called compartments.
- Compartments with regards to virtualization as defined and used in the PP are called zones in this TOE. This refinement is restricted to chapters 1, 6 and 7.
- The following assignment statement "[assignment: the authorized identified roles, or users that satisfy the following rules: [rules that define when a user is allowed to override the default values]" as defined and used in FAU and FMT SFRs have been replaced with "users that are authorized to assume identified roles" in this ST. This refinement appears in chapter 6.
- This rationale is to attest that the A.CONNECT, A.PEER.FUNC, A.PEER.MGT assumptions satisfy the requirements specified in chapter 8 of base BSI OS PP for the claimed client-server implementations of remote audit storage and Kerberos functionality.

Security Objectives Rationale

This chapter provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. This chapter demonstrates the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

Security Objectives Rationale Relating to Threats

*Table **14*** below provides a mapping of the objects to the threats they counter.

Table 14 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ACCESS.COMM A threat agent might access a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system or masquerade as another remote trusted IT system.	O.TRUSTED_CHANNEL The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.	The threat of accessing a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system is removed by O.TRUSTED_CHANNEL requiring that the TOE implements a trusted channel between itself and a remote trusted IT system protecting the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.
	OE.REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.	The threat of accessing a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system is removed by OE.REMOTE requiring that those systems providing the functions required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
T.ACCESS.TSFDATA A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.	O.CRYPTO.NET The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.	The threat of accessing TSF data without proper authorization is removed by O.CRYPTO.NET requiring cryptographically-protected communication channels for data including TSF data controlled by the TOE in transit between trusted IT systems.
	O.DISCRETIONARY.ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	The threat of accessing TSF data without proper authorization is removed by O.DISCRETIONARY.ACCESS requiring that data, including TSF data stored with the TOE, have discretionary access control protection.
	O.SUBJECT.COM	The threat of accessing TSF data

Threats	Objectives	Rationale
	The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.	without proper authorization is removed by O.SUBJECT.COM requiring the TSF to mediate communication between subjects.
T.ACCESS.TSFFUNC A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.	O.CRYPTO.NET The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.	The threat of accessing TSF functions without proper authorization is removed by O.CRYPTO.NET requiring cryptographically-protected communication channels to limit which TSF functions are accessible to external entities.
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.	The threat of accessing TSF functions without proper authorization is removed by O.MANAGE requiring that only authorized users utilize management TSF functions.
	O.ROLE.MGMT The TOE must allow security management actions based on roles to be assigned to different users.	The threat of an attacker accessing TSF functions without proper authorization is additionally covered due to extended functionality by O.ROLE.MGMT requiring the TOE to allow security management actions based on roles to be assigned to different users.
T.ACCESS.USERDATA A threat agent might gain access to user data stored, processed, or transmitted by the TOE without being appropriately authorized according to the TOE security policy.	O.CRYPTO.NET The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.	The threat of accessing user data without proper authorization is removed by O.CRYPTO.NET requiring cryptographically-protected communication channels for data including TSF data controlled by the TOE in transit between trusted IT systems.
	O.DISCRETIONARY.ACCESS The TSF must control access of subjects and/or users to named resources based	The threat of accessing user data without proper authorization is removed by O.DISCRETIONARY.ACCESS

Threats	Objectives	Rationale
	on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	requiring that data, including TSF data stored with the TOE, have discretionary access control protection.
	O.SUBJECT.COM The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.	The threat of accessing user data without proper authorization is removed by O.SUBJECT.COM requiring the TSF to mediate communication between subjects.
T.IA.MASQUERADE A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.	O.I&A The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.	The threat of masquerading as an unauthorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources is removed by O.I&A requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only.
T.IA.USER A threat agent might gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.	O.I&A The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.	The threat of accessing user data, TSF data, or TOE resources without being identified and authenticated is removed by O.I&A requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only.
T.RESTRICT.NETTRAFFIC A threat agent might get access to information or transmit information to other recipients via network communication channels without authorization for this communication attempt by the information flow control policy.	O.NETWORK.FLOW The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE and the TOE itself in accordance with its security policy.	The threat of accessing information or transmitting information to other recipients via network communication channels without authorization for this communication attempt is removed by O.NETWORK.FLOW requiring the TOE to mediate the communication between itself and remote entities in accordance with its security policy.
T.ROLE.SNOOP An attacker might obtain the rights granted to a role that was delegated to another user.	O.ROLE.DELEGATE The TOE must allow roles assigned to users for performing security-relevant management tasks to be delegated to other users in accordance with the security policy.	The threat of an attacker obtaining the rights granted to a role that was delegated to another user is removed by O.ROLE.DELEGATE requiring the TOE to allow delegation of roles to other users in accordance with the security policy.
T.ROLE.DELEGATE An attacker might delegate rights granted to a role that he does not possess or that he is not allowed to delegate.	O.ROLE.DELEGATE The TOE must allow roles assigned to users for performing security-relevant management tasks to be delegated to other users in accordance with the	The threat of an attacker delegating rights granted to a role that he does not possess or that he is not allowed to delegate is removed by O.ROLE.DELEGATE requiring the

Threats	Objectives	Rationale
	security policy.	TOE to allow roles assigned to users for performing security-relevant management tasks to be delegated.
T.DATA_NOT_SEPARATED The TOE might not adequately separate data on the basis of its sensitivity label, thereby allowing information to flow illicitly from or to users.	O.LS.CONFIDENTIALITY The TOE will control information flow between entities and resources based on the sensitivity labels of users and resources.	The threat of not adequately separating data on the basis of its sensitivity label, thereby allowing information to flow illicitly from or to users, is removed by O.LS.CONFIDENTIALITY requiring the TOE to control information flow between entities and resources, based on the sensitivity labels of users and resources.
T.ACCESS.COMPENV A threat agent might utilize or modify the runtime environment of other compartments in an unauthorized manner.	O.COMP.IDENT For each access request, the TOE is able to identify the compartment requesting to access resources, objects, or information.	The threat of utilizing or modifying the runtime environment of compartments executing on behalf of other users is removed by O.COMP.IDENT requiring the TOE to identify the compartment requesting to access resources, objects, or information for each access request.
	O.COMP.RESOURCE_ACCESS The TOE will control access of compartments to objects and resources under its control based on: security attributes of the objects; security attributes of the compartment that attempts to access the object; and the type of access attempted. The rules that determine access may be based on the value of other TSF data. Access must be controlled down to individual compartments and objects.	The threat of utilizing or modifying the runtime environment of compartments executing on behalf of other users is removed by O.COMP.RESOURCE_ACCESS requiring the TOE to control access of compartments to objects and resources under its control.
T.INFOFLOW.COMP A threat agent might get access to information without authorization by the information flow control policy.	O.COMP.IDENT For each access request, the TOE is able to identify the compartment requesting to access resources, objects, or information.	The threat of accessing information without authorization by the information flow control policy is removed by O.COMP.IDENT requiring the TOE to identify the compartment requesting to access resources, objects, or information for each access request.
	O.COMP.INFO_FLOW_CTRL The TOE will control information flow between compartments under the control of the TOE, based on security attributes of these compartments and potentially other TSF data (e.g., security attributes of objects). This information flow control policy must be able to allow the isolation of individual	The threat of accessing information without authorization by the information flow control policy is removed by O.COMP.INFO_FLOW_CTRL requiring the TOE to control information flow between compartments under the control of the TOE based on security attributes of these compartments and potentially

Threats	Objectives	Rationale
	compartments from other compartments controlled by the TOE.	other TSF data.
T.COMM.COMP A threat agent might access the data communicated between compartments or between a compartment and an external entity to read or modify the transferred data.	O.COMP.IDENT For each access request, the TOE is able to identify the compartment requesting to access resources, objects, or information.	The threat of accessing the data communicated between compartments or between a compartment and an external entity is removed by O.COMP.IDENT requiring the TOE to identify the compartment requesting to access resources, objects, or information for each access request.
	O.COMP.RESOURCE_ACCESS The TOE will control access of compartments to objects and resources under its control based on: security attributes of the objects; security attributes of the compartment that attempts to access the object; and the type of access attempted. The rules that determine access may be based on the value of other TSF data. Access must be controlled down to individual compartments and objects.	The threat of accessing the data communicated between compartments or between a compartment and an external entity is removed by O.COMP.RESOURCE_ACCESS requiring the TOE to control access of compartments to objects and resources under its control.

Every Threat is mapped to one or more Objectives in the *Table **14*** above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

Security Objectives Rationale Relating to Policies

Table 15 below gives a mapping of policies and the objectives that support them.

Table 15 Policies: Objectives Mapping

Policies	Objectives	Rationale
P.ACCOUNTABILITY The users of the TOE shall be held accountable for their security-relevant actions within the TOE.	O.AUDITING The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the	The policy to hold users accountable for their security-relevant actions within the TOE is implemented by O.AUDITING providing the TOE with audit functionality.

Policies	Objectives	Rationale
	identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.	
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.	The policy to hold users accountable for their security-relevant actions within the TOE is implemented by O.MANAGE allowing the management of this function.
P.APPROVE Specific rights assigned to users and controlled by the TSF shall only be exercisable if approved by a second user.	O.ROLE.APPROVE The TOE must prevent the execution of user actions allowed by a specific right until a second user with a different right approves this action.	The policy that specific rights assigned to users shall only be exercisable when approved by a second user is implemented by O.ROLE.APPROVE requiring the TOE to prevent the execution of user actions allowed by a specific right until a second user with a different right approves this action.
P.CLEARANCE The system must limit information flow between protected resources and authorized users based on whether the user's sensitivity label is appropriate for the labeled information.	O.LS.CONFIDENTIALITY The TOE will control information flow between entities and resources based on the sensitivity labels of users and resources.	The policy to limit information flow between protected resources and authorized users based on whether the user's sensitivity label is appropriate for the labeled information is implemented by O.LS.CONFIDENTIALITY requiring the TOE to control information flow between entities and resources based on the sensitivity labels of users and resources.
P.I&A.REMOTE Remote trusted IT systems shall be able to obtain identification and authentication decisions from the TOE based on credentials transmitted by a remote trusted IT system to the TOE.	O.I&A.MULTIPLE The TOE shall allow the concurrent use of multiple identification and authentication mechanisms implementing the identification and authentication policy.	The policy to obtain identification and authentication decisions from the TOE based on credentials transmitted by a remote trusted IT system to the TOE is implemented by O.I&A.MULTIPLE allowing the concurrent use of multiple identification and authentication mechanisms implementing the identification and authentication policy.
	O.I&A.REMOTE The TOE shall allow remote trusted IT systems to transmit user credentials to the TOE. Using these credentials, the TOE shall perform a local identification and authentication policy decision, and	The policy to obtain identification and authentication decisions from the TOE based on credentials transmitted by a remote trusted IT system to the TOE is implemented by O.I&A.REMOTE allowing remote trusted IT systems to

Policies	Objectives	Rationale
	then communicate this decision back to one or more trusted IT systems, based on the identification and authentication policy.	transmit user credentials to the TOE, which uses these credentials to perform a local identification and authentication policy decision. This decision is communicated back to one or more remote trusted IT systems based on the identification and authentication policy.
P.LABELED_OUTPUT The beginning and end of all paged, hardcopy output must be marked with sensitivity labels that properly represent the sensitivity label of the output.	O.LS.PRINT The TOE will provide the capability to mark printed output with accurate labels based on the sensitivity label of the subject requesting the output.	The policy to provide the capability to mark printed output with accurate labels based on the sensitivity label of the user causing the output is implemented by O.LS.PRINT providing the capability to mark printed output with accurate labels based on the sensitivity label of the user causing the output.
P.RESOURCE_LABELS All resources accessible by subjects and all subjects must have associated labels identifying the sensitivity levels of data contained therein.	O.LS.LABEL The TOE will provide the capability to label all subjects, and all objects accessible by subjects, to restrict information flow based on the sensitivity labels.	The policy that resources accessible by subjects and all subjects must have associated labels identifying the sensitivity levels of data contained therein is implemented by O.LS.LABEL providing the capability to label all subjects and all objects accessible by subjects, to restrict the information flow based on the sensitivity labels.
P.USER Authority shall only be given to users who are trusted to perform the actions correctly.	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.	The policy to match the trust given to a user and the actions the user is given authority to perform is implemented by O.MANAGE allowing appropriately-authorized users to manage the TSF.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. Specifically, all network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system, as such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted; DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly; and users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	The policy to match the trust given to a user and the actions the user is given authority to perform is implemented by OE.INFO_PROTECT, which requires that users are trusted to use the protection mechanisms of the TOE to protect their data.

Policies	Objectives	Rationale
P.USER_CLEARANCE All users must have a clearance level identifying the maximum sensitivity levels of data they may access.	O.LS.CONFIDENTIALITY The TOE will control information flow between entities and resources based on the sensitivity labels of users and resources.	The policy that users must have a clearance level identifying the maximum sensitivity levels of data they may access is implemented by O.LS.CONFIDENTIALITY requiring the TOE to control information flow between entities and resources based on the sensitivity labels of users and resources.
	O.LS.LABEL The TOE will provide the capability to label all subjects, and all objects accessible by subjects, to restrict information flow based on the sensitivity labels.	The policy that users must have a clearance level identifying the maximum sensitivity levels of data they may access is implemented by O.LS.LABEL ensuring that objects and subjects can be labeled such that the TOE can restrict information flow based on those labels.

Every policy is mapped to one or more Objectives in the Table 15 above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.AUTHUSER 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.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.	The assumption on authorized users to possess the necessary authorization to access at least some of the information managed by the TOE and to act in a cooperating manner in a benign environment is covered by OE.ADMIN ensuring that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. Specifically, all network and peripheral cabling must be	The assumption on authorized users to possess the necessary authorization to access at least some of the information managed by the TOE and to act in a cooperating manner in a benign environment is covered by OE.INFO_PROTECT requiring that

Assumptions	Objectives	Rationale
	approved for the transmittal of the most sensitive data held by the system, as such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted; DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly; and users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly and that users are authorized to access parts of the data maintained by the TOE.
A.CONNECT All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.	OE.REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.	The assumption that all connections to and from remote trusted IT systems and between physically separated parts of the TSF not protected by the TSF itself are physically or logically protected is covered by OE.REMOTE requiring that remote trusted IT systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.TRUSTED.IT.SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	The assumption that all connections to and from remote trusted IT systems and between physically separated parts of the TSF not protected by the TSF itself are physically or logically protected is covered by OE.TRUSTED.IT.SYSTEM demanding the physical and logical protection equivalent to the TOE.
A.DETECT Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.	OE.INSTALL Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.	The assumption that modification or corruption of security-enforcing or security-relevant files will be detected by an administrative user is covered by OE.INSTALL requiring an administrative user to ensure that the TOE is distributed, installed, and configured in a secure manner supporting the security mechanisms provided by the TOE.

Assumptions	Objectives	Rationale
	OE.MAINTENANCE Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.	The assumption that modification or corruption of security-enforcing or security-relevant files will be detected by an administrative user is covered by OE.MAINTENACE requiring an administrative user to ensure that the diagnostics facilities are invoked at every scheduled preventative maintenance period, verifying the correct operation of the TOE.
	OE.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 (security) compromise is achieved.	The assumption that modification or corruption of security-enforcing or security-relevant files will be detected by an administrative user is covered by OE.RECOVER requiring an administrative user to ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
A.MANAGE The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.	The assumptions on the TOE security functionality being managed by one or more trustworthy individuals is covered by OE.ADMIN requiring trustworthy personnel managing the TOE.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. Specifically, all network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system, as such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted; DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly; and users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	The assumptions on the TOE security functionality being managed by one or more trustworthy individuals is covered by OE.INFO_PROTECT requiring personnel to ensure that information is protected in an appropriate manner.

Assumptions	Objectives	Rationale
	OE.INSTALL Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.	The assumptions on the TOE security functionality being managed by one or more trustworthy individuals is covered by OE.INSTALL requiring personnel to ensure that components that comprise the system are distributed, installed, and configured in a secure manner supporting the security mechanisms provided by the TOE.
	OE.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 (security) compromise is achieved.	The assumptions on the TOE security functionality being managed by one or more trustworthy individuals is covered by OE.RECOVER requiring personnel to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
A.PEER.FUNC All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.	OE.TRUSTED.IT.SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	The assumption on all remote trusted IT systems to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality is covered by OE.TRUSTED.IT.SYSTEM requiring that the remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.
A.PEER.MGT All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.	OE.TRUSTED.IT.SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	The assumption on all remote trusted IT systems to be under the same management control and operate under security policy constraints compatible with those of the TOE is covered by OE.TRUSTED.IT.SYSTEM requiring that these remote trusted IT systems are under the same management domain as the TOE, and are managed based on the same rules and policies applicable to the TOE.
A.PHYSICAL It is assumed that the IT	OE.INFO_PROTECT Those responsible for the TOE must	The assumption on the IT environment to provide the TOE with appropriate

Assumptions	Objectives	Rationale
environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	establish and implement procedures to ensure that information is protected in an appropriate manner. Specifically, all network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system, as such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted; DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly; and users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	physical security, commensurate with the value of the IT assets protect by the TOE is covered by OE.INFO_PROTECT requiring the approval of network and peripheral cabling.
	OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.	The assumption on the IT environment to provide the TOE with appropriate physical security, commensurate with the value of the IT assets protect by the TOE is covered by OE.PHYSICAL requiring physical protection.
A.TRAINEDUSER Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.	The assumptions on users to be sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data is covered by OE.ADMIN requiring competent personnel managing the TOE.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. Specifically, all network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system, as such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted; DAC protections on	The assumptions on users to be sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data is covered by OE.INFO_PROTECT requiring that those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner and that users are trained to exercise control over their own data.

Assumptions	Objectives	Rationale
	security-relevant files (such as audit trails and authentication databases) shall always be set up correctly; and users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	

Every assumption is mapped to one or more Objectives in the Table 16 above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

Rationale for Extended Security Functional Requirements

Table 17 presents the rationale for the inclusion of the extended functional and assurance requirements found in the BSI OSPP.

Table 17 Rationale for Extended Requirements

Extended Requirement	Identifier	Rationale
FCS_RNG.1	Generation of random numbers	The quality of the random number generator is defined using this SFR. The quality metric required in FCS_RNG.1.2 is detailed in the German Scheme AIS 20 and AIS 31.
FDP_RIP.3	Full residual information protection of resources	FDP_RIP.3 addresses the problem of resources implemented in main memory that may be allocated to and de-allocated from subjects or users. Unless those resources lose their content automatically as part of the de-allocation and re-allocation process, they must be subject to a process that prepares them for re-use by rendering the previous content unavailable to the subject or user to which it is next allocated. An example is main memory that has been allocated to a subject; this memory must be cleared before it can be re-allocated to a subject with different security attributes (for example a subject operating on behalf of a different user). This preparation prevents the passing of security-critical information via this resource, since such unregulated passing would potentially allow the subject or user to which the memory is next allocated to user this information to violate the security policy. Typical examples of such critical information that may be passed via resources not prepared for re-use are passwords or cryptographic keys.
FIA_UAU.8	Authentication policy decisions	FIA_UAU.8 specifies the authentication policy decision mechanism whereby other entities can send a request to the TOE, the TOE processes the request according to the local authentication policy, and the TOE returns the result to other entities based on specified rules. This SFP is intended for TOEs acting as an authentication server for other, usually remote, trusted IT systems.
FIA_UID.3	Identification policy decisions	FIA_UID.3 specifies the identification policy decision mechanism whereby other entities can send a request to the TOE, the TOE process the request according to the local identification policy, and the TOE returns the result to other entities based on specified rules. This SFR is intended for TOEs acting as an identification server for other, usually remote, trusted IT systems.

Extended Requirement	Identifier	Rationale
FIA_USB.2	Enhanced user-subject binding	An operating system may derive subject security attributes from other TSF data that are not directly user security attributes. An example is the point-of-entry the user has used to establish the connection. An access control policy may also use this subject security attribute within its access control policy, allowing access to critical objects only when the user has connected through specific ports-of-entry.

Rationale for Extended TOE Security Assurance Requirements

No extended SARs have been defined for this ST.

Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

Rationale for Security Functional Requirements of the TOE Objectives

Table 18 below shows a mapping of the objectives and the SFRs that support them.

Table 18 Objectives: SFRs Mapping

Objective	Applicable SFRs	Rationale
O.AUDITING The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to	FAU_GEN.1 Audit Data Generation	The events to be audited are defined in [FAU_GEN.1] and are associated with the identity of the user that caused the event [FAU_GEN.2]. Authorized users are provided the capability to read the audit records [FAU_SAR.1], while all other users are denied access to the audit records [FAU_SAR.2]. The authorized user must have the capability to specify which audit records are generated [FAU_SEL.1]. The TOE prevents the audit log from being modified or deleted [FAU_STG.1] and ensures that the audit log is not lost due to resource shortage [FAU_STG.3, FAU_STG.3 (Remote), FAU_STG.4]. To support
	FAU_GEN.2 User Identity Association	
	FAU_SAR.1 Audit Review	
	FAU_SAR.2 Restricted Audit Review	
	FAU_SEL.1 Selective Audit	
	FAU_STG.1 Protected Audit Trail Storage	
	FAU_STG.3 Action in Case of Possible Data Loss	
	FAU_STG.3 (Remote)	

Objective	Applicable SFRs	Rationale
compromise.	FAU_STG.4 Prevention of Audit Data Loss	auditing, the TOE is able to maintain proper time stamps [FPT_STM.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
	FDP_RIP.2 Full Residual Information Protection	
	FDP_RIP.3 Full Residual Information Protection of Resources	
	FPT_SMT.1 Reliable Timestamp	
O.COMP.IDENT For each access request, the TOE is able to identify the compartment requesting to access resources, objects, or information.	FIA_UID.2(VIRT) User identification before any action	The identification of compartments to support the information flow control and access control policies is established with [FIA_UID.2 (VIRT)].
O.COMP.INFO_FLOW_CTRL The TOE will control information flow between compartments under the control of the TOE, based on security attributes of these compartments and potentially other TSF data (e.g., security attributes of objects). This information flow control policy must be able to allow the isolation of individual compartments from other compartments controlled by the TOE.	FDP_ETC.2(VIRT) Export of user data with security attributes	The information flow control policy covering the runtime of the compartments is specified with [FDP_IFC.2 (VIRT)], and [FDP_IFF.1 (VIRT)]. As the TOE shall allow export of data belonging to compartments, the TOE assigns the security attributes for enforcing the information flow control policy to the communicated data as specified with [FDP_ETC.2(VIRT)], [FDP_ITC.2(VIRT)], and [FPT_TDC.1(VIRT)]. Management of the security attributes for the information flow control policy is specified with [FMT_MSA.1 (VIRT-CIFCP)], and [FMT_MSA.3 (VIRT-CIFCP)] as well as FMT_MTD.1 (VIRT-COMP).
	FDP_IFC.2(VIRT) Complete Information Flow Control	
	FDP_IFF.1(VIRT) Simple Security Attributes	
	FDP_ITC.2(VIRT) Import of User Data with Security Attributes	
	FMT_MSA.1(VIRT_CIFCP) Management of Security Attributes	
	FMT_MSA.3(VIRT_CIFCP) Static Attribute Initialisation	
	FMT_MTD.1(VIRT_COMP) Management of TSF Data	
	FPT_TDC.1(VIRT) Inter-TSF basic TSF Data Consistency	
O.COMP.RESOURCE_ACCESS The TOE will control access of compartments to objects and resources under its control based on: security attributes of the	FDP_ACC.2(VIRT) Complete access control	The access control policy for the resources belonging to the different compartments is defined with [FDP_ACC.2 (VIRT)], and [FDP_ACF.1 (VIRT)].
	FDP_ACF.1(VIRT) Security Attribute Based Access Control	

Objective	Applicable SFRs	Rationale
objects; security attributes of the compartment that attempts to access the object; and the type of access attempted. The rules that determine access may be based on the value of other TSF data. Access must be controlled down to individual compartments and objects.	FDP_ETC.2(VIRT) Export of user data with security attributes	As the TOE shall allow export of data belonging to compartments, the TOE assigns the security attributes for enforcing the access control policy to the communicated data as specified with [FDP_ETC.2(VIRT)], [FDP_ITC.2(VIRT)], and [FPT_TDC.1(VIRT)]. Management of the security attributes for the access control policy is specified with [FMT_MSA.1 (VIRT-CACP)], and [FMT_MSA.3 (VIRT-CACP)] as well as FMT_MTD.1 (VIRT-COMP).
	FDP_ITC.2(VIRT) Import of User Data with Security Attributes	
	FMT_MSA.1(VIRT_CACP) Management of Security Attributes	
	FMT_MSA.3(VIRT_CACP) Static Attribute Initialisation	
	FMT_MTD.1(VIRT_COMP) Management of TSF Data	
	FPT_TDC.1(VIRT) Inter-TSF basic TSF Data Consistency	
O.CRYPTO.NET The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.	FCS_CKM.1(DSA) Cryptographic Key Generation	The cryptographically-protected network protocol [FCS_COP.1(NET)] is supported by the generation of symmetric keys [FCS_CKM.1(SYM), FCS_RNG.1], as well as asymmetric keys [FCS_CKM.1(RSA), FCS_CKM.1(DSA), FCS_RNG.1)]. As part of the cryptographic network protocol, the TOE securely exchanges the symmetric key with a remote trusted IT system [FCS_CKM.2 (NET)]. The TOE ensures that all keys are zeroized upon de-allocation [FCS_CKM.4]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
	FCS_CKM.1(RSA) Cryptographic Key Generation	
	FCS_CKM.1(SYM) Cryptographic Key Generation	
	FCS_CKM.2(NET) Cryptographic Key Distribution	
	FCS_CKM.4 Cryptographic Key Destruction	
	FCS_COP.1(NET) Cryptographic Operation	
	FCS_RNG.1 Random Number Generator	
	FDP_RIP.2 Full Residual Information Protection	
	FDP_RIP.3 Full Residual Information Protection of Resources	
O.DISCRETIONARY.ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each	FDP_ACC.1(PSO) Subset access control	The TSF must control access to resources based on the identity of users that are allowed to specify which resources they want to access for storing their data. The access control policy must
	FDP_ACF.1(PSO) Security Attribute Based Access Control	

Objective	Applicable SFRs	Rationale
access mode which users/subjects are allowed to access a specific named object in that access mode.	FDP_ITC.2 Import of User Data with Security Attributes	have a defined scope of control [FDP_ACC.1(PSO)]. The rules for the access control policy are defined [FDP_ACF.1(PSO)]. When import of user data is allowed, the TOE must ensure that user data security attributes required by the access control policy are correctly interpreted [FDP_ITC.2, FPT_TDC.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
	FDP_RIP.2 Full Residual Information Protection	
	FDP_RIP.3 Full Residual Information Protection of Resources	
	FPT_TDC.1 Inter-TSF basic TSF Data Consistency	
O.I&A The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.	FDP_RIP.2 Full residual information protection	The TSF must ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process [FIA_UID.1, FIA_UAU.1]. Multiple I&A mechanisms are allowed as specified in [FIA_UAU.5]. To ensure authorized access to the TOE, authentication data is protected [FIA_ATD.1(HU), FIA_UAU.7]. Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB.2]. The appropriate strength of the authentication mechanism is ensured [FIA_SOS.1]. To support the strength of authentication methods, the TOE is capable of identifying and reacting to unsuccessful authentication attempts [FIA_AFL.1]. In addition, user-initiated and TSF-initiated session locking [FTA_SSL.1, FTA_SSL.2] protect the authenticated user's session. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3] are present.
	FDP_RIP.3 Full Residual Information Protection of Resources	
	FIA_AFL.1 Authentication Failure Handling	
	FIA_ATD.1(HU) User Attribute Definition	
	FIA_SOS.1 Verification of Secrets	
	FIA_UAU.1 Timing of Authentication	
	FIA_UAU.5 Multiple Authentication Mechanisms	
	FIA_UAU.7 Protected Authentication Feedback	
	FIA_UID.1 Timing of Identification	
	FIA_USB.2 Enhanced User-Subject Binding	
	FTA_SSL.1 TSF-Initiated Session Locking	
	FTA_SSL.2 User-Initiated Locking	

Objective	Applicable SFRs	Rationale
O.I&A.MULTIPLE The TOE shall allow the concurrent use of multiple identification and authentication mechanisms implementing the identification and authentication policy.	FIA_UAU.5 Multiple authentication mechanisms	The TOE shall provide multiple I&A policies specified with [FIA_UAU.5] from the OSPP base: at least one for local I&A and one for remote I&A.
O.I&A.REMOTE The TOE shall allow remote trusted IT systems to transmit user credentials to the TOE. Using these credentials, the TOE shall perform a local identification and authentication policy decision, and then communicate this decision back to one or more trusted IT systems, based on the identification and authentication policy.	FIA_ATD.1(EIA) User attribute definition	The remotely-triggerable I&A policy is defined with the identification mechanism [FIA_UID.3], the authentication mechanism [FIA_UAU.8], and the specification of the security attributes applicable to this policy [FIA_ATD.1 (EIA)]. The management aspect of this I&A policy is covered with [FMT_MTD.1 (EIA)].
	FIA_UAU.8(EIA) Authentication policy decisions	
	FIA_UID.3(EIA) Identification policy decisions	
	FMT_MTD.1(EIA) Management of TSF data	
O.LS.CONFIDENTIALITY The TOE will control information flow between entities and resources based on the sensitivity labels of users and resources.	FDP_ETC.2(LS) Export of user data with security attributes	The information flow control policy is defined by specifying the subjects, objects, security attributes, and rules in [FDP_IFC.2(LS), FDP_IFF.2(LS)]. Supportive to the enforcement of the policy are the automated label assignment when exporting data [FDP_ETC.2 (LS)] and during the import of data[FDP_ITC.1(LS), FDP_ITC.2(LS)]. For assigning labels to imported data, the label information transmitted with the data must be interpretable by the TOE [FPT_TDC.1 (LS)].
	FDP_IFC.2(LS) Complete information flow control	
	FDP_IFF.2(LS) Hierarchical security attributes	
	FDP_ITC.1(LS) Import of user data without security attributes	
	FDP_ITC.2(LS) Import of user data with security attributes	
	FPT_TDC.1(LS) Inter-TSF basic TSF data consistency	
O.LS.LABEL The TOE will provide the capability to label all subjects, and all objects accessible by subjects, to restrict information flow based on the sensitivity labels.	FDP_ITC.1(LS) Import of user data without security attributes	The assignment of labels to users is performed during user-subject binding [FIA_USB.1 (LS)] with security attributes maintained by the TOE [FIA_ATD.1 (LS)]. Object labels are assigned to objects when importing them into the TOE [FDP_ITC.1 (LS), FDP_ITC.2 (LS), FPT_TDC.1 (LS)]. The management of labels is allowed for the TOE with [FMT_MSA.1 (LS), FMT_MSA.3
	FDP_ITC.2(LS) Import of user data with security attributes	
	FIA_ATD.1(LS) User attribute definition	
	FIA_USB.1(LS) User-subject binding	
	FMT_MSA.1(LS)	

Objective	Applicable SFRs	Rationale
	Management of security attributes	(LS)].
	FMT_MSA.3(LS) Static attribute initialisation	
	FPT_TDC.1(LS) Inter-TSF basic TSF data consistency	
O.LS.PRINT The TOE will provide the capability to mark printed output with accurate labels based on the sensitivity label of the subject requesting the output.	FDP_ETC.2(LS) Export of user data with security attributes	The addition of label information on exported data during printing is governed by [FDP_ETC.2 (LS)].
O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.	FMT_MSA.1(PSO) Management of object security attributes	The TOE provides management interfaces globally defined in [FMT_SMF.1] for: - the access control policies [FMT_MSA.1(PSO), FMT_MSA.1(TSO), FMT_MSA.3(PSO), FMT_MSA.3(TSO)]; - the information flow control policy [FMT_MSA.3(NI), FMT_MTD.1(NI)]; - the auditing aspects [FMT_MTD.1(AE), FMT_MTD.1(AS), FMT_MTD.1(AT), FMT_MTD.1(AF)]; - the identification and authentication aspects [FMT_MTD.1(IAT), FMT_MTD.1(IAF), FMT_MTD.1(IAU)]. Persistently stored user data is stored either in hierarchical or relational fashion, which implies an inheritance of security attributes from parent object [FMT_MSA.4 (PSO)]. The rights management for the different management aspects is defined with [FMT_SMR.1]. The management interfaces for the revocation of user and object attributes is provided with FMT_REV.1 (OBJ) and FMT_REV.1 (USR)].
	FMT_MSA.1(TSO) Management of object security attributes	
	FMT_MSA.3(NI) Static attribute initialisation	
	FMT_MSA.3(PSO) Static attribute initialisation	
	FMT_MSA.3(TSO) Static attribute initialisation	
	FMT_MSA.4(PSO) Security attribute value inheritance	
	FMT_MTD.1(AE) Management of TSF data	
	FMT_MTD.1(AF) Management of TSF data	
	FMT_MTD.1(AS) Management of TSF data	
	FMT_MTD.1(AT) Management of TSF data	
	FMT_MTD.1(IAF) Management of TSF data	
	FMT_MTD.1(IAT) Management of TSF data	
	FMT_MTD.1(IAU) Management of TSF data	
	FMT_MTD.1(NI) Management of TSF data	

Objective	Applicable SFRs	Rationale
	FMT_REV.1(OBJ) Revocation	
	FMT_REV.1(USR) Revocation	
	FMT_SMF.1 Specification of management functions	
	FMT_SMR.1 Security roles	
O.NETWORK.FLOW The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE and the TOE itself in accordance with its security policy.	FDP_IFC.2(NI) Complete information flow control	The network information flow control mechanism controls the information flowing between different entities [FDP_IFC.2 (NI)]. The TOE implements a rule-set governing the information flow [FDP_IFF.1 (NI)]. To facilitate the information flow control, the information must be identified [FIA_UID.1] based on security attributes the TOE can maintain [FIA_ATD.1 (TU)]. The TOE must ensure that security attributes of the network data required by the information flow control policy are correctly interpreted [FDP_ITC.2, FPT_TDC.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
	FDP_IFF.1(NI) Simple security attributes	
	FDP_ITC.2 Import of user data with security attributes	
	FDP_RIP.2 Full residual information protection	
	FDP_RIP.3 Full residual information protection of resources	
	FIA_ATD.1(TU) User attribute definition	
	FIA_UID.1 Timing of identification	
	FPT_TDC.1 Inter-TSF basic TSF data consistency	
O.ROLE.APPROVE The TOE must prevent the execution of user actions allowed by a specific right until a second user with a different right approves this action.	FMT_MTD.1(AM-AP) Management of TSF data	The approval mechanism for roles is defined with [FMT_MTD.1 (AM-AP)], supported by management of the approval mechanism, i.e., specification of which roles can approve which operations [FMT_MTD.1 (AM-MA)].
	FMT_MTD.1(AM-MA) Management of TSF data	
O.ROLE.DELEGATE The TOE must allow roles assigned to users for performing security-relevant management tasks to be delegated to other users in accordance with the security policy.	FMT_MTD.1(AM-MD) Management of TSF data	The delegation of roles is defined and specified in [FMT_MTD.1 (AM-MD)].

Objective	Applicable SFRs	Rationale
O.ROLE.MGMT The TOE must allow security management actions based on roles to be assigned to different users.	FMT_MTD.1(AM-MR) Management of TSF data	The definition and management of rights based on roles is defined in [FMT_MTD.1 (AM-MR)].
O.SUBJECT.COM The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.	FDP_ACC.1(TSO) Subset access control	The TSF must control the exchange of data using transient storage objects between subjects based on the identity of users. The access control policy must have a defined scope of control [FDP_ACC.1 (TSO)]. The rules for the access control policy are defined [FDP_ACF.1 (TSO)]. When import of user data is allowed, the TOE must ensure that user data security attributes required by the access control policy are correctly interpreted [FDP_ITC.2, FPT_TDC.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
	FDP_ACF.1(TSO) Security attribute based access control	
	FDP_ITC.2 Import of user data with security attributes	
	FDP_RIP.2 Full residual information protection	
	FDP_RIP.3 Full residual information protection of resources	
	FPT_TDC.1 Inter-TSF basic TSF data consistency	
O.TRUSTED_CHANNEL The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.	FTP_ITC.1 Inter-TSF trusted channel	The TOE provides a trusted channel protecting communication between a remote trusted IT system and itself [FTP_ITC.1].

Security Assurance Requirements Rationale

EAL4, augmented with ALC_FLR.3 was chosen to provide a moderate- to high-level of assurance that is consistent with the requirements of the BSI Operating System Protection Profile, version 2.0. The chosen assurance level is appropriate with the threats defined for the environment. At EAL4+, the TOE will have undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of enhanced-basic.

In addition, due to operating systems being complex systems which are the basis for almost all applications in today's IT environments, the BSI OS PP requires the inclusion of ALC_FLR.3 mandating the developer to provide security-relevant patches in due time after the identification of a flaw.

The augmentation of ASE_CCL.1.10C is considered to include certain requirements, such as statements marked as "ST-Author Note" and the specification given in chapter 8 of the BSI Operating System Protection Profile, version 2.0 with which ST must comply. These requirements specify conditional requirements that only apply when the TOE shows special properties or mechanisms. The CC does not define such conditional statement, which are therefore introduced by the BSI Operating System Protection Profile, version 2.0.

Dependency Rationale

The SFRs in this ST satisfy most of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 19 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the Table 19 indicates, most dependencies have been met.

FMT_MSA.3 (NI): FMT_MTD.1 (NI) is specified to require the management of security attributes for the Network Information Flow Control Policy, just as a potential FMT_MSA.1 (NI) would have been specified. However, the Network Information Flow Control Policy is not required to be enforced when managing the security attributes, as the management aspect of the network information flow control functionality is not protected by the network information flow control mechanism. Therefore, FMT_MSA.1 is not applicable and is replaced with FMT_MTD.1 (NI).

Table 19 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SEL.1	FAU_GEN.1	✓	
	FMT_MTD.1	✓	This is satisfied by FMT_MTD.1(AE)
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.3	FAU_STG.1	✓	
FAU_STG.3(Remote)	FAU_STG.1	✓	
FAU_STG.4	FAU_STG.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.1(DSA)	FCS_CKM.4	✓	
	FCS_COP.1	✓	This is satisfied by FCS_COP.1 (NET)
FCS_CKM.1(RSA)	FCS_CKM.4	✓	
	FCS_COP.1	✓	This is satisfied by FCS_COP.1(NET)
FCS_CKM.1(SYM)	FCS_CKM.4	✓	
	FCS_COP.1	✓	This is satisfied by FCS_COP.1(NET)
FCS_CKM.2(NET)	FCS_CKM.1	✓	This is satisfied by FCS_CKM.1(DSA), FCS_CKM.1(RSA), FCS_CKM.1(SYM)
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	This is satisfied by FCS_CKM.1(SYM)
FCS_COP.1(NET)	FCS_CKM.1	✓	This is satisfied by FCS_CKM.1(DSA), FCS_CKM.1(RSA), FCS_CKM.1(SYM)
	FCS_CKM.4	✓	
FCS_RNG.1	No dependencies	✓	
FDP_ACC.1(PSO)	FDP_ACF.1	✓	This is satisfied by FDP_ACF.1(PSO)
FDP_ACC.1(TSO)	FDP_ACF.1	✓	This is satisfied by FDP_ACF.1(TSO)
FDP_ACC.2(VIRT)	FDP_ACF.1	✓	This is satisfied by FDP_ACF.1(VIRT)
FDP_ACF.1(PSO)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(PSO)

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_MSA.3	✓	This is satisfied by FMT_MSA.3(PSO)
FDP_ACF.1(TSO)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(TSO)
	FMT_MSA.3	✓	This is satisfied by FMT_MSA.3(TSO)
FDP_ACF.1(VIRT)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.2(VIRT), which is hierarchical to FDP_ACC.1
	FDP_MSA.3	✓	This is satisfied by FMT_MSA.3(VIRT-CACP)
FDP_ETC.2(LS)	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(LS), which is hierarchical to FDP_IFC.1
FDP_ETC.2(VIRT)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.2(VIRT), which is hierarchical to FDP_ACC.1
	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(VIRT), which is hierarchical to FDP_IFC.1
FDP_IFC.2(LS)	FDP_IFF.1	✓	This Is satisfied by FDP_IFF.2(LS), which is hierarchical to FDP_IFF.1
FDP_IFC.2(NI)	FDP_IFF.1	✓	This is satisfied by FDP_IFF.1(NI)
FDP_IFC.2(VIRT)	FDP_IFF.1	✓	This is satisfied by FDP_IFF.1(VIRT)

SFR ID	Dependencies	Dependency Met	Rationale
FDP_IFF.1(NI)	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(NI), which is hierarchical to FDP_IFC.1
	FMT_MSA.3	✓	This is satisfied by FMT_MSA.3(NI)
FDP_IFF.1(VIRT)	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(VIRT), which is hierarchical to FDP_IFC.1
	FDP_MSA.3	✓	This is satisfied by FMT_MSA.3(VIRT-CIFCP).
FDP_IFF.2(LS)	FDP_IFC.1(LS)	✓	This is satisfied by FDP_IFC.2(LS), which is hierarchical to FDP_IFC.1
	FMT_MSA.3	✓	This is satisfied by FMT_MSA.3(LS)
FDP_ITC.2	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(PSO), FDP_ACC.1(TSO)
	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(NI), which is hierarchical to FDP_IFC.1
	FPT_TDC.1	✓	
	FTP_ITC.1	✓	
FDP_ITC.2(LS)	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(LS), which is hierarchical to FDP_IFC.1
	FDP_ITC.1	✓	This is satisfied by FDP_ITC.1(LS)

SFR ID	Dependencies	Dependency Met	Rationale
	FPT_TDC.1	✓	This is satisfied by FPT_TDC.1(LS)
FDP_ITC.2(VIRT)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.2(VIRT), which is hierarchical to FDP_ACC.1
	FDP_IFC.1	✓	This is resolved by FDP_IFC.2(VIRT), which is hierarchical to FDP_IFC.1
	FPT_TDC.1	✓	
	FTP_ITC.1	✓	
FDP_RIP.2	No dependencies	✓	
FDP_RIP.3	No dependencies	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_ATD.1(EIA)	No dependencies	✓	
FIA_ATD.1(HU)	No dependencies	✓	
FIA_ATD.1(LS)	No dependencies	✓	
FIA_ATD.1(TU)	No dependencies	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UAU.8(EIA)	FTP_ITC.1	✓	
FIA_UID.1	No dependencies	✓	
FIA_UID.2(VIRT)	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UID.3(EIA)	FTP_ITC.1	✓	
FIA_USB.1(LS)	FIA_ATD.1	✓	This is satisfied by FIA_ATD.1(LS)
FIA_USB.2	FIA_ATD.1	✓	This is satisfied by FIA_ATD.1(HU)
FMT_MSA.1(LS)	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(LS), which is hierarchical to FDP_IFC.1
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(PSO)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(PSO)
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(TSO)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(TSO)
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(VIRT-CACP)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.2(VIRT), which is hierarchical to FDP_ACC.1
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(VIRT-CIFCP)	FDP_IFC.1	✓	This is satisfied by FDP_IFC.2(VIRT), which is hierarchical to FDP_IFC.1
	FMT_SMF.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMR.1	✓	
FMT_MSA.3(LS)	FMT_MSA.1	✓	This is satisfied by FMT_MSA.1(LS)
	FMT_SMR.1	✓	
FMT_MSA.3(NI)	FMT_MSA.1	No	Satisfied instead with FMT_MTD.1(NI)
	FMT_SMR.1	✓	
FMT_MSA.3(PSO)	FMT_MSA.1	✓	This is satisfied by FMT_MSA.1(PSO)
	FMT_SMR.1	✓	
FMT_MSA.3(TSO)	FMT_MSA.1	✓	This is satisfied by FMT_MSA.1(TSO)
	FMT_SMR.1	✓	
FMT_MSA.3(VIRT-CACP)	FMT_MSA.1	✓	This is satisfied by FMT_MSA.1(VIRT-CACP)
	FMT_SMR.1	✓	
FMT_MSA.3(VIRT-CIFCP)	FMT_MSA.1	✓	This is satisfied by FMT_MSA.1(VIRT_CIFCP)
	FMT_SMR.1	✓	
FMT_MSA.4(PSO)	FDP_ACC.1	✓	This is satisfied by FDP_ACC.1(PSO)
FMT_MTD.1(AE)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(AF)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MTD.1(AM-AP)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(AM-MA)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(AM-MD)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(AM-MR)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(AS)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(AT)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(EIA)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(IAF)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(IAT)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(IAU)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(NI)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_REV.1(OBJ)	FMT_SMR.1	✓	
FMT_REV.1(USR)	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	No dependencies	✓	
	No dependencies	✓	
FPT_TDC.1	No dependencies	✓	
FPT_TDC.1(LS)	No dependencies	✓	
FPT_TDC.1(VIRT)	No dependencies	✓	
FTA_SSL.1	FIA_UAU.1	✓	
FTA_SSL.2	FIA_UAU.1	✓	
FTP_ITC.1	No dependencies	✓	

CHAPTER

A Glossary

Acronyms

This annex and Table 20 define the acronyms and terms used throughout this document.

Table 20 Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
ACK	Acknowledge
ACL	Access Control List
AES	Advanced Encryption Standard
AI	Automated Installer
AM	Advanced Management
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CC	Common Criteria
CD	Compact Disk
CD-ROM	Compact Disk-Read Only Memory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CTR	Counter
DAC	Discretionary Access Control
DES	Data Encryption Standard
DOS	Disk Operating System
DVD	Digital Versatile Disk

Acronym	Definition
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EIA	Extended Identification and Authentication
FIFO	First-In, First-Out special file
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standards Publication
GCM	Galios/Counter Mode
GID	Group Identifier
GNOME	GNU Network Object Model Environment
GNU	GNU's Not Unix
GSS	Generic Security Services
GSSAPI	Generic Security Services Application Programming Interface
GUI	Graphical User Interface
HMAC-SHA	Hash-Based Message Authentication Code-Secure Hash Algorithm
ICMP	Internet Control Message Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPC	Inter-process Communication
IPsec	Internet Protocol Security
IPS	Image Packing System
ISO	International Organization for Standardization
IT	Information Technology
JCE	Java Cryptography Extension
KMF	Key Management Feature
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LS	Labeled Security
MAC	Mandatory Access Control

Acronym	Definition
MD5	Message Digest 5
NFS	Network File System
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OSPP	Operating System Protection Profile
PAM	Pluggable Authentication Module
PCFS	Personal Computer File System
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PSO	Persistent Storage Object
RBAC	Role-Based Access Control
RAM	Random Access Memory
RFC	Request for Comments
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman algorithm
SAR	Security Assurance Requirement
SASL	Simple Authentication and Security Lager
SCI	Sierra's Creative Interpreter
SCTP	Stream Control Transmission Protocol
SDP	Socket Direct Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMF	Service Management Facility
SPARC	Scalable Processor Architecture
SSH	Solaris Secure Shell
ST	Security Target
SYN	Synchronize
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple Data Encryption Standard

Acronym	Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSO	Transient Storage Object
TSP	TOE Security Policy
TX	Trusted Extensions
UDFS	Universal Disk Format System
UDP	User Datagram Protocol
UFS	Unix File System
UID	User Identifier
US	United States (of America)
VIRT	Virtualization
VLAN	Virtual Local Area Network
VM	Virtual Machine
WAN	Wide Area Network
ZFS	Zettabyte File System