Xceedium GateKeeper Version 5.2.1 Security Target

Version 3.0

February 3, 2011

Prepared for:
Xceedium, Inc.
30 Montgomery Street
Jersey City, NJ 07302

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

.

LIST OF TABLES

.

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. Xceedium provides the TOE, which is Xceedium GateKeeper Version 5.2.1. The TOE is an Information Technology (IT) management tool that provides the ability to remotely maintain multiple network devices (server, routers, and platforms). The TOE is accessed via any Java enabled browser. The communication between the TOE and the browser is protected by SSL. The TOE provides the administrators with the interfaces to manage users, devices, and access policies.

The Security Target contains the following additional sections:

- Section 2 – TOE Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Problem Definition
  This section details the expectations of the environment, the threats that are countered by Xceedium and it environment and the organizational policy that the Xceedium must fulfill.
- Section 4 –Security Objectives
  This section details the security objectives of the Xceedium and its environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for Xceedium and details the assurance requirements for EAL4.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the Xceedium that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any Protection Profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Xceedium GateKeeper Version 5.2.1 Security Target

ST Version – Version 3.0

ST Date – February 3, 2011

TOE Identification – Xceedium GateKeeper Version 5.2.1

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 2, September 2007.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 2, September 2007.

.

- Part 3 Conformant
- Evaluation Assurance Level 4 augmented with ALC_FLR.2 (EAL4 with ALC_FLR.2)

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Acronyms

The acronyms used within this Security Target:

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AGD	Administrator Guidance Document
ANSI	American National Standards Institute
CC	Common Criteria
CPU	Central Processing Unit
DDR	Double Data Rate
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
GUI	Graphical User Interface
IP	Internet Protocol
IPC	Interprocess Communication

IT	Information Technology
KVM	Keyboard-Video-Mouse
LCD	Liquid Crystal Display
NTP	Network Time Protocol
PBX	Private Branch Exchange
PERL	Practical Extraction and Report Language
PP	Protection Profile
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
RSA	Rivest, Shamir, & Adleman (encryption algorithm)
SBC	Single Board Computer
SNMP	Simple Network Management Protocol
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control
TOE	Target of Evaluation
TSF	TOE Security Functions
VNC	Virtual Network Connection

2. TOE Description

The Target of Evaluation (TOE) is the Xceedium appliance Xceedium GateKeeper 5.2.1, hereafter referred to as the TOE. The product is designed by Xceedium, located at, 30 Montgomery Street, Jersey City, NJ 07302.

2.1 TOE Overview

The GateKeeper product provides FIPS-validated SSL[1]-secured, in-band and out-of-band management and monitoring of networking equipment, UNIX, Linux, Macintosh and Windows servers, as well as remote power-management to either turn on, off, or reboot any attached device. Its purpose is to enable purchasers to remotely manage the activities of users from a central point to anywhere in the heterogeneous IT infrastructure, without modification of legacy systems.

The GateKeeper TOE consists of an appliance and zero or more backend agents running on Windows or UNIX servers. Management of the TOE is performed using a Java enable browser over an SSL connection. The following sections detail the TOE components and their capabilities.

2.2 TOE Description

The TOE is designed to reside between untrusted users on an unprotected network and a protected network. Its purpose is to limit access to the resources on the protected network and provide for management of those resources from a centralized location. The TOE is composed of the four main components described below:

[1] Reference: Certificate number 813

.

1. GateKeeper Appliance - The GateKeeper appliance is a rack mounted network device. It provides access control to the devices located on the protected network and provides management interfaces for its policies. The appliance contains an internal database to store its configuration information, access policies, and audit records. The appliance also contains a web server to communicate with administrators managing the appliance via browsers. Within the web server, the appliance implements SSLv3 to support its management connections.
2. GateKeeper Agents (Socket Filter Agent) – The GateKeeper agents can run on Windows, UNIX or Linux servers located on the protected network. The purpose of the agents is to further limit access from servers on the protected network, to other devices within the protected network in order to enforce audit and access policies. Once users gain access via the policies supported on the appliance, the agents can further limit access by restricting which ports may be utilized to create outbound connections to other resources within the protected environment.
3. Management Interface – Management of the TOE is performed by administrators using a Java enabled web browser. The TOE provides a set of graphical interfaces in which to perform the management functions for the appliance and agents. The TOE also provides an SNMP interface to allow Administrators to retrieve management configuration information.
4. GateKeeper Client - A set of Java Applets used by end users to access the GateKeeper Appliance. The clients do not enforce any security policies.

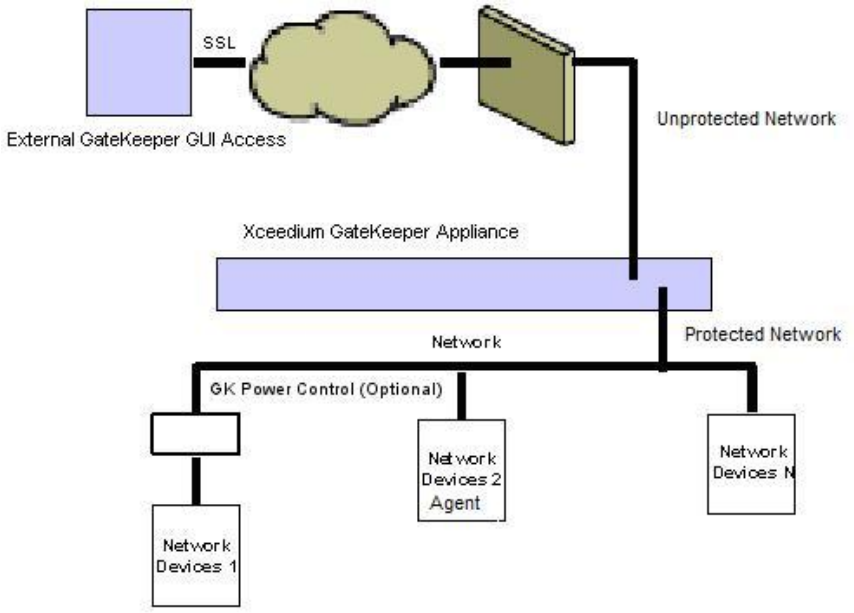

Figure 1: Xceedium GateKeeper TOE in its environment

The appliance requires all users to perform authentication to it using an identifier and a password. Once successful logon has occurred, administrators can perform management. When users log into the appliance they are doing so in order to access a device (e.g., service, network device) located on the protected network behind the appliance. Users are subject to an access control policy enforced by the appliance when they attempt to access a protected resource.

The access control policy enforced on users is based upon user identity and services provided by the backend device. Users are given access to particular services on specific devices. The set of services that are available for control are:

- ***VNC* (options: Standard, Linux, Web version)**– graphical access to a device (requires a VNC Server service to be installed and running on the device)
- ***Telnet*** – standard, unsecured Telnet access to a device

.

- ***SSH –*** secured, in-band console access to a device (requires a SSH v1 or v2 server (daemon) to be installed and running on the device)
- ***SSH2Telnet –*** allows secured access to a Telnet-enabled device by using the secure shell protocol for communications between the client and the GateKeeper appliance, All subsequent connections from the GateKeeper appliance to the target Telnet server (deamon) will be using the plain text Telnet protocol. This methodology allows for strict enforcement of only approved encrypted protocols outside of the protected network.
- ***R DP –*** Remote desktop connection (required the remote desktop connection enabled)
- ***Out-of-Band*** – serial (RS-232) console access of a device. (requires a network enabled serial concentrator supporting reverse telnet or reverse SSH)
- ***Power*** – remote boot (power on/off/reboot) of a device. (requires a network enabled "smart power" concentrator supporting reverse telnet or reverse ssh)
- ***Service*** – Other TCP/UDP services can also be defined by the authorized administrator for execution by end users. These services may include: fat client access such as SQL query frontends, mainframe clients, or any proprietary applications which use TCP or UDP connections. Note: As these services are defined and provided by the administrator, they are outside the scope of the TOE

Users are granted one or more services to a device. When a user attempts to access a device, the request is checked against the permitted services.

With the support of the Socket Filter Agents, the appliance also supports a Socket Filter List in addition to the device access policy. This access policy permits an administrator to establish a set of sockets that are permitted for use on a backend device protected by the TOE by way of a proprietary agent installed on the target device. The administrator has the option of establishing a white list which results in only those sockets included on the white list are permitted or a black list which permits all but the listed sockets. At any period of time, there is only a white list or black list active for a user and device pair. However multiple users may connect to the same target device each with their own discrete policy being enforced.

In addition to the Socket filtering policy enforcement, the appliance maintains an option for enforcing policy on systems protected by the TOE where installation of an agent is impossible or impractical (i.e. hardened appliances such as switches or routers). Enforcement of Command Filters is achieved by intercepting keystrokes and allows the administrator to define commands, strings or regular expressions that users can or cannot execute against a device. The administrator has the option of establishing a white list which results in only those commands or strings included on the white list are permitted or a black list which permits all but the listed commands or strings. At any period of time, there is only a white list or black list active for a user and device pair. However multiple users may connect to the same target device each with their own discrete policy being enforced. Command filters are only applied to CLI-based applets: SSH, Telnet, and SSH to Telnet. Command filter policies applied to any other applets are ignored and not enforced.

Users and administrators access the TOE, but only administrators can manage TOE security functions. Administrators may view logins, user sessions, and reporting; set configuration parameters and conduct maintenance tasks; utilize management features; and set associations between users and devices. All administrative actions are mediated by the TOE. The TOE provides the ability to record administrative sessions. These recordings are stored externally in an administrator provisioned server (either NFS or CIFS). The GateKeeper keeps a local SHA1 hash of all the session files for integrity checks during session recording playbacks.

2.3 Product Features

The TOE implements the following features:

- Web-based access to establish VNC, Telnet, SSH, and standard operating system specific GUI sessions to network devices over TCP/IP.
- Browser access to all types of graphical and text based sessions using Windows, UNIX.
- Supported target system platforms: Windows server, Sun Solaris, HP/UX, and AIX

.

- Supported network devices: File Servers, Desktop PC's, Routers, switches, terminal servers, private branch exchange (PBX), and other network enabled devices.
- Authentication via TOE web server
- Multiple text based UNIX sessions to access a network device
- SSL user communication
- Single Access Port to network devices
- Web interface GUI for administrators and users
- Logging for monitored events
- Failover (Clustering) - This feature involves using multiple GateKeepers as a cluster
- NTP – the TOE can optionally synch with a time server to maintain its clock
- SSL VPN – This access method is available in FIPS mode
- Monitor – Used for tracking user sessions

The following product features are not part of the evaluated configuration:

- RADIUS and RSA Authentication Methods - These methods are not available in FIPS mode.
- External Logging - This feature is not available in FIPS mode.

2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The TOE consists of the GateKeeper appliance, agents, and management interface. The appliance has three network interfaces – one to the unprotected network, an Agent interface and one to the protected network where it enforces a device access control policy. All users connect to the appliance using SSL via the unprotected network.

A third interface for the appliance is its LCD Panel and four configuration buttons on the front of the appliance. This external interface allows for basic network configuration of the device out of the box. Once the appliance basic network configuration has been completed via the LCD Panel and buttons that interface with the configuration firmware, the device is rebooted, and the web-based configuration of network parameters are completed via an Internet Browser (any Java-enabled web browser). Once in the evaluated configuration the appliance is assumed to be in a protected environment and the LCD Panel and buttons are not used and do not need any further description.

Agents reside on either Windows or UNIX servers on the protected network. The agents do not interface directly with users. The access control policy is pushed to the agent from the appliance where it is then applied.

The TOE web server provides an administrative interface for all TOE management functions called the Administrative Modules. From this GUI interface, the administrator manages user access. The actual browser and user workstation supporting the browser are not part of TOE.

All servers and devices on the protected network are in the IT Environment.

2.4.1.1 Hardware Specifications

The following is a list of hardware used on the appliance.

Chassis	1U IPC Chassis
Power Supply	250W Power Supply Unit (PSU)
System Board	Single Board Computer (SBC) Intel Chipset
CPU (Model Specific)	Intel Core2 Duo 2.13Ghz

.

Memory (Model Specific)	4GB DDR
Disk (Model Specific)	32GB Solid-State Drive (SSD)
Ports	6 GigE interfaces
Additional Storage	32GB Solid-State Drive (SSD)
Display	LCD Display

2.4.2 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces.

2.4.2.1 Security Audit

The TOE Web Server generates audit records related to the authentication and management of the TOE that are stored and protected in an internal database. The TOE records attempts to access itself, such as successful and failed authentication attempts, as well as the actions taken by users once authenticated. The appliance generates audit records for all access control decisions it makes. All auditable actions can be found in Active Logins, Sessions, Logs and Report interface. The Logs Report Parameters screen allows administrator selection of the specific report information to be generated.

2.4.2.2 Cryptographic Support

The TOE has been FIPS 140-2 evaluated and is configured to run in FIPS mode in the evaluated configuration. The TOE implements SSL to all user communication with the TOE. Users establish an SSL connection to the TOE before submitting a username/password to perform authentication. Users then use the SSL channel to transmit all information to the TOE. The TOE also supports x509v3 certificate generate and validation.

2.4.2.3 User Data Protection

The TOE enforces an access control policy that controls access between users and devices. Access to devices is limited based upon the user identifier associated with the requestor and device service access list. A user can access a given service on a given device if the device service access control list specifically allows access to the requested service for the device. The TOE also supports two additional policies that can be configured in addition to the basic device access policy. The first policy limits access to particular sockets on devices and the second perform keyword filtering on device commands.

2.4.2.4 Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any access to the system is granted. The TOE supports password, client certificate, and external LDAP authentication. The TOE also maintains security privileges used for role assignments.

2.4.2.5 Security Management

An authorized administrator is any user that has an administrative privilege. Users with no administrative privileges are simply called users. The TOE is managed through the Administrative modules (Config, Services, Sessions, Users, Devices, Policy), accessed via a SSL web-based interface. Through this interface all TOE management can be performed, including user management and the configuration of IT devices access functions. This interface is restricted to authorized administrators, which provides the administrator the ability to set user attributes and privileges, as well as assign privileges for different levels of administrative access.

Administration functions are done using PERL scripts which are triggered by input via the GUI. A spadmin daemon accepts input from specific functions on the web server to control system configuration parameters. Scripts operate the features of the optional TOE power, console, and IP based KVM device components.

.

2.4.2.6 Protection of Security Functions

The TOE is a hardware appliance that contains a custom operating system that runs in firmware, and supports only trusted processes. The GateKeeper appliance provides no file abstractions or permanent storage for user access for "executables" to remain for further execution. Furthermore, the TOE has been carefully designed to offer well-defined interfaces that ensure that access to protected resources is subject to the applicable GateKeeper security policies. The agents are service processes on Windows or daemon processes on UNIX. In either case, the operating system provides a separate address for the agent to run. Additionally, all communication between the appliance and agent is protected using SSL. If the TOE is configured in a cluster and one GateKeeper becomes unavailable, another GateKeeper will automatically start receiving all requests and will maintain a secure state. The TOE also generates timestamps for use within the audit trail or can optionally get time from an ntp server.

2.5 Guidance Documentation

Xceedium provides administrator guidance to end users. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install Xceedium products in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration. The guidance document also explains how to securely administer the product. The guidance documentation is

- Xceedium GateKeeper V 5.2.1 Administration Guide

3. Security Problem Definition

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

3.1 Threats to Security

3.1.1 TOE Threats

T.AUDIT_COMPROMISE A user may cause audit data to be inappropriately accessed (viewed, modified or deleted),

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.TSF_COMPROMISE A malicious user may cause the TOE, configuration data, or sensitive user data to be inappropriately accessed (viewed, modified or deleted) allowing a breach in the TSF security policies.

T.UNAUTH_ACCESS A user may gain unauthorized access to devices.

3.2 Organization Security Policies

P.MANAGE The TOE must provide authorized administrators with utilities to effectively manage the security functions of the TOE

P.PROTECT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

P.AUDIT Users of the system shall be accountable for their security relevant actions within the system.

.

3.3 Secure Usage Assumptions

3.3.1 Physical Assumptions

A.LOCATE The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.CONNECT All network traffic will be configured to pass through the TOE.

3.3.2 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4. Security Objectives

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

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data as defined by the administrator.

O.AUDIT The TOE must record the security relevant actions of users of the TOE and must present this information in a readable format to authorized administrators.

O.AUDIT_PROTECTION The TOE must provide the capability to protect audit information

O.MANAGE The TOE must provide services that allow effective management of its functions and data.

O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.RECOVER_STATE The TOE must provide the ability to maintain a secure state in the case the TOE becomes inoperable

O.TIME The TOE must provide reliable time stamps for audit records.

4.2 Security Objectives for the Environment

OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

OE.PERSON Authorized users of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.

OE.PHYCAL Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack that might compromise the TOE security objectives.

.

5. IT Security Requirements

This section provides a list of all security functional requirements for the TOE.

5.1 TOE Security Functional Requirements

The following table lists the SFRs.

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation
	FAU_SAR.1 Audit Review
	FAU_SAR.2: Restricted audit review
	FAU_SAR.3: Selectable audit review
	FAU_STG.1 Protected audit trail storage
Cryptographic Support (FCS)	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1: Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1Subset Access Control
	FDP_ACF.1Security attribute based access control
Identification and authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5 Multiple Authentication mechanisms
	FIA_UID.2 User identification before any action
Security management (FMT)	Management of security attributes – service associations (FMT_MSA.1)
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1(a)Management of TSF data (security-relevant privileges)
	FMT_MTD.1(b) Management of TSF data (authentication data)
	FMT_MTD.1(c) Management of TSF data (timestamp)
	FMT_MTD.1(d) Management of TSF data (user identity)
	FMT_MTD.1(e) Management of TSF data (audit data)
	FMT_MTD.1(f) Management of TSF data (certificate management)
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_FLS.1 Failure with preservation of secure state
	FPT_ITT.1: Basic Internal Transfer Protection
	FPT_STM.1 Reliable time stamps

Table 1 Security Functional Components

5.1.1 Audit Requirements

5.1.1.1 Audit Data Generation (FAU_GEN.1)

5.1.1.1.1 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 **[*not specified*]** level of audit; and

c) **[All authentication attempts to the TOE**

d) **Adding and Removing user accounts**

e) **Changes to authentication data (passwords)**

f) **Access Control decisions**

g) **Changes to user attributes and privileges]**.

5.1.1.1.2 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, **[no other additional information]**

5.1.1.2 Audit Review (FAU_SAR.1)

5.1.1.2.1 FAU_SAR.1.1

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

5.1.1.2.2 FAU_SAR.1.2

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

5.1.1.3 Restricted audit review (FAU_SAR.2)

5.1.1.3.1 FAU_SAR.2.1

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

5.1.1.4 Selectable audit review (FAU_SAR.3)

5.1.1.4.1 FAU_SAR.3.1

The TSF shall provide the ability to apply **[searches]** of audit data based on **[any audit record contents]**

.

5.1.1.5 Protected audit trail storage (FAU_STG.1)

5.1.1.5.1 FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

5.1.1.5.2 FAU_STG.1.2

The TSF shall be able to **[*prevent*]** unauthorised modifications to the stored audit records in the audit trail.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[listed below]** and specified cryptographic key sizes **[specified for each algorithm]** that meet the following: **[standards noted for each algorithm]**

a.) **AES 128 bits or 256 bits (FIPS 197)**
b.) **3DES 168 bits (ANSI X9.52)**
c.) **RSA 1024 bits or 2048 bits (FIPS 186-3)**

5.1.2.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zero out the memory locations containing raw key values immediately after session disconnection**] that meets the following: [**none**].

5.1.2.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform **[hash generation, encryption, decryption]** in accordance with a specified cryptographic algorithm **[listed below]** and cryptographic key sizes **[specified for each algorithm]** that meet the following: **[standards noted for each algorithm].**

a.) **Hash generation SHA-1 (FIPS PUB 180-1, ANSI X9.30 Part 2**
b.) **Encryption/Decryption 3DES 168 (ANSI X9.52), AES 128 bits or 256 bits (FIPS 197)**
c.) **Digital Signature RSA 1024 bits or 2048 bits (ANSI X9.31, FIPS 186-3)**
d.) **X 509v3 Certificate generation 1024 bits or 2048 bits (RFC 3280)**

5.1.3 User Data Protection (FDP)

5.1.3.1 Subset access control (FDP_ACC.1)

5.1.3.1.1 FDP_ACC.1.1

The TSF shall enforce the **[Device Access Control SFP]** on **[subjects: users, objects: devices, operations: access to devices]**.

5.1.3.2 Security attribute based access control (FDP_ACF.1)

5.1.3.2.1 FDP_ACF.1.1

The TSF shall enforce the **[Device Access Control SFP]** to objects based on the following;

[Subject (users): user identity and

Object (devices): service access control list, socket policy list, command filter].

.

5.1.3.2.2 FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[To access a device, a user must have access to the service, the socket and the command if applicable based upon the following rules:**

1. **A user can access a given service on a given device if the device service access control list specifically allows access to the requested service;**
2. **If a Socket Policy exists for a device identifying the user one of the following rules is applied:**
    a. **If a white list exists for a device and user, the user can access a particular socket if that socket is on the white list; otherwise access to the socket is denied.**
    b. **If a black list exists for a device and user, the user is denied access to a particular socket if that socket is on the black list; otherwise access to the socket is permitted**

    Else, if no Socket Policy exists, access to the socket is permitted.
3. **If a Command Filter exists for a device identifying the user one of the following rules is applied:**
    a. **If a white list exists for a device and user, the user can use a particular command on a device if that command is on the white list; otherwise the command is denied.**
    b. **If a black list exists for a device and user, the user is denied access to the command on the device if that command is on the black list; otherwise the command is permitted**

    Else, if no Command Filter exists, the command on the device is permitted].

5.1.3.2.3 FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[no additional rules]**.

5.1.3.2.4 FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the **[no additional rules]**.

5.1.4 Identification and authentication (FIA)

5.1.4.1 User attribute definition (FIA_ATD.1)

5.1.4.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: **[user identity, authentication data, and security privileges]**.

Application Note: Security privileges are used in the assignment of roles to a user. Roles are composed of sets of privileges.

5.1.4.2 User authentication before any action (FIA_UAU.2)

5.1.4.2.1 FIA_UAU.2.1

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

.

5.1.4.3 Multiple Authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide a [**password, an external LDAP server, and client certificates**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**rule that each user can be configured for one or more authentication mechanisms and any must be successful for authentication to be successful.]**.

5.1.4.4 User identification before any action (FIA_UID.2)

5.1.4.4.1 FIA_UID.2.1

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

5.1.5 Security management (FMT)

5.1.5.1 Management of security attributes – service associations (FMT_MSA.1)

5.1.5.1.1 FMT_MSA.1.1

The TSF shall enforce the **[Device Access Control SFP]** to restrict the ability to **[create, *modify, delete*]** the security attributes **[service access control list, socket policy list, command filter]** to **[authorized administrators]**.

5.1.5.2 Static attribute initialization (FMT_MSA.3)

5.1.5.2.1 FMT_MSA.3.1

The TSF shall enforce the **[Device Access Control SFP]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

5.1.5.2.2 FMT_MSA.3.2

The TSF shall allow the **[authorized administrators]** to specify alternative initial values to override the default values when an object or information is created.

5.1.5.3 Management of TSF data (FMT_MTD.1(a)) (Security-Relevant Privileges)

5.1.5.3.1 FMT_MTD.1.1(a)

The TSF shall restrict the ability to **[*modify, delete, clear*]** the **[security-relevant privileges for users]** to **[authorized administrators]**.

5.1.5.4 Management of TSF data (FMT_MTD.1(b)) (Authentication data)

5.1.5.4.1 FMT_MTD.1.1(b)

The TSF shall restrict the ability to **[*modify*]** the **[authentication data]** to **[authorized administrators and users authorized to modify their own authentication data]**.

.

5.1.5.5 Management of TSF data (FMT_MTD.1(c)) (Timestamp)

5.1.5.5.1 FMT_MTD.1.1(c)

The TSF shall restrict the ability to **[*modify*]** the **[timestamp]** to **[the Configurator]**.

5.1.5.6 Management of TSF data (FMT_MTD.1(d)) (User Identity)

5.1.5.6.1 FMT_MTD.1.1(d)

The TSF shall restrict the ability to **[create]** the **[user identifier]** to **[authorized administrators]**.

5.1.5.7 Management of TSF data (FMT_MTD.1(e)) (Audit data)

5.1.5.7.1 FMT_MTD.1.1(e)

The TSF shall restrict the ability to **[manage]** the **[audit data]** to **[authorized administrators]**

5.1.5.8 Management of TSF data (FMT_MTD.1(f)) (Certificate Management)

5.1.5.8.1 FMT_MTD.1.1(f)

The TSF shall restrict the ability to **[manage]** the **[x.509v3 certificates]** to **[authorized administrators].**

5.1.5.9 Specification of Management Functions (FMT_SMF.1)

5.1.5.9.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: **[**

a) **Management of access control (Device access control policy)**

b) **Management of user attributes**

c) **Management of audit functions**

d) **Management of the timestamp**

e) **Management of x509v3 Certificates**

f) **Recording and viewing of administrative sessions]**.

5.1.5.10 Security roles (FMT_SMR.1)

5.1.5.10.1 FMT_SMR.1.1

The TSF shall maintain the roles **[authorized administrators, Configurator, and users authorized to update authentication data]**.

5.1.5.10.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

.

5.1.6 Protection of the TOE security functions (FPT)

5.1.6.1 Failure with preservation of secure state (FPT_FLS.1)

5.1.6.1.1 FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [**if a GateKeeper fails when it is clustered, a GateKeeper within the cluster will preserve the secure state**].

5.1.6.2 Basic internal TSF Data Transfer Protection (FPT_ITT.1)

5.1.6.2.1 FPT_ITT.1.1

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE through the use of the TSF-provided cryptographic services: **[encryption and decryption]**.

5.1.6.3 Reliable time stamps (FPT_STM.1)

5.1.6.3.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
Development (ADV)	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
Guidance Documents (AGD)	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.4: Production support, acceptance procedures and automation
	ALC_CMS.4: Problem tracking CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
Tests (ATE)	ATE_COV.2: Analysis of coverage
	ATE_DPT.2: Testing: security enforcing modules
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.3: Focused vulnerability analysis

Table 2 EAL 4 augmented with ALC_FLR.2 Assurance Components

.

5.2.1 Development (ADV)

5.2.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.
ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3c The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
ADV_ARC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 Complete functional specification (ADV_FSP.4)

ADV_FSP.4.1d The developer shall provide a functional specification.
ADV_FSP.4.2d The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.4.1c The functional specification shall completely represent the TSF.
ADV_FSP.4.2c The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.4.3c The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.4.4c The functional specification shall describe all actions associated with each TSFI.
ADV_FSP.4.5c The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.
ADV_FSP.4.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.4.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 Implementation representation of the TSF (ADV_IMP.1)

ADV_IMP.1.1d The developer shall make available the implementation representation for the entire TSF.
ADV_IMP.1.2d The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.
ADV_IMP.1.1c The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2c The implementation representation shall be in the form used by the development personnel.
ADV_IMP.1.3c The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.
ADV_IMP.1.1e The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

5.2.1.4 Basic modular design (ADV_TDS.3)

ADV_TDS.3.1d The developer shall provide the design of the TOE.
ADV_TDS.3.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.3.1c The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.3.2c The design shall describe the TSF in terms of modules.
ADV_TDS.3.3c The design shall identify all subsystems of the TSF.
ADV_TDS.3.4c The design shall provide a description of each subsystem of the TSF.

.

ADV_TDS.3.5c The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.3.6c The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
ADV_TDS.3.7c The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.
ADV_TDS.3.8c The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, and interaction with called interfaces to other modules.
ADV_TDS.3.9c The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
ADV_TDS.3.10c The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.
ADV_TDS.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.3.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Production support, acceptance procedures and automation (ALC_CMC.4)

ALC_CMC.4.1d The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.4.2d The developer shall provide the CM documentation.
ALC_CMC.4.3d The developer shall use a CM system.
ALC_CMC.4.1c The TOE shall be labelled with its unique reference.
ALC_CMC.4.2c The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3c The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4c The CM system shall provide automated measures such that only authorised changes are made to the configuration items.
ALC_CMC.4.5c The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6c The CM documentation shall include a CM plan.
ALC_CMC.4.7c The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8c The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9c The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10c The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.
ALC_CMC.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 Problem tracking CM coverage (ALC_CMS.4)

ALC_CMS.4.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.4.1c The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.
ALC_CMS.4.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.4.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2d The developer shall use the delivery procedures.
ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.
ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

.

5.2.3.5 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall document flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5c The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.6 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.
ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.7 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1d The developer shall identify each development tool being used for the TOE.
ALC_TAT.1.2d The developer shall document the selected implementation-dependent options of each development tool.
ALC_TAT.1.1c Each development tool used for implementation shall be well-defined.
ALC_TAT.1.2c The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.
ALC_TAT.1.3c The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.
ALC_TAT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 Testing: security enforcing modules (ATE_DPT.2)

ATE_DPT.2.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.2.1c The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.
ATE_DPT.2.2c The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.
ATE_DPT.2.3c The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.
ATE_DPT.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Focused vulnerability analysis (AVA_VAN.3)

AVA_VAN.3.1d The developer shall provide the TOE for testing.
AVA_VAN.3.1c The TOE shall be suitable for testing.
AVA_VAN.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.3.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.3.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

.

AVA_VAN.3.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

FAU_GEN.1 Audit Data Generation, FAU_STG.1 Audit storage protection

The TOE can generate audit records of all the events listed in section 5.1.1.1 as part of the definition of FAU_GEN.1.1 with the exception of the event for audit startup and shutdown as auditing is always on. Audit records include at least event time and date, event type, subject identity and outcome (success or failure) as well as other data specific to the report type such as port, status, address etc.. The audit trail is protected so that only an authorized administrator can read the audit records. All audit trail records are stored in the TOE internal database. The Administration Modules are the only interface to the audit trail and its access is restricted. Only authorized administrators are able to view these audit records through the Administration Modules using the Sessions (Sessions -> logs) module. Only the authorized administrator is able to purge the audit trail.

The TOE generates audit data for all authentication attempts to the TOE, including successful and unsuccessful attempts. The audit function also generates records for the creation, removal and modification of user accounts, network device access attempts, as well as the security-relevant privileges assigned to the accounts. The TOE also records all changes to authentication data, whether changed by an administrator or the user.

Administrators have access to a sessions screen portion of the Administrative Modules from which three types of reports can be –Active Logins, Sessions, or Logs.

- Active Logins (under Sessions-> Manage Sessions link)– lists the users that are presently logged in to the TOE
- Sessions (under Sessions ->Overview link)– lists the sessions that are presently in use to manage devices from the TOE
- Logs (under Sessions -> Logs link) – lists the logs of previous transaction made to and/or from the TOE.

FAU_SAR.1 Audit Review, FAU_SAR.3 Selectable Audit Review

The TOE presents the audit data in a format viewable by authorized administrators for review. The Report screen displays the generated report. The authorized administrator has the ability to search the audit trail based upon any field in the audit data,

6.1.2 Cryptographic Support

FCS_COP.1 Cryptographic Operation, FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, FPT_ITT.1 Basic internal TSF Data Transfer Protection

The TOE uses TLSv1/SSLv3 to protect communication between users, administrators, and the TOE itself. The connection is protected using AES or 3DES encryption/decryption and SHA-1 hashing invoked according to the SSL protocol. The authorized administrator sets the encryption policy. SSL connections are authenticated using certificates. Certificates are managed internally to the TOE web server and are protected from user access. Session keys are destroyed by zeroing memory after the user disconnects from the TOE session. Key Generation currently perform in the TOE are public-private RSA keys, AES-256 Credential Storage key" RSA keys are perform upon request of the UI triggered by the User. Credential Storage key is done on first boot-up.

.

The TOE supports Public Key Infrastructure (PKI) authentication by using x509 certificates. Clients present their certificates to the TOE and the TOE uses its internal Certificate chain and Certificate Revocation list to validate the user. The TOE can generate RSA certificate requests, as well as self-signed certificate using X509v3 standard and the RSA algorithms. Certificates can be uploaded to the TOE in PEM and DER format.

6.1.3 User Data Protection

FDP_ACC.1 Subset Access Control (Device Access Control)

The TOE controls access to the devices by limiting access to users for all requests made to devices.

FDP_ACF.1 Security Attribute based access control (Device Access Control)

The TOE protects devices that are logically located behind it on a network. The TOE maintains an association between users and devices, called a device association. Users are associated with particular devices and for particular services on those devices; this association is maintained in a service access control list. The TOE grants access to a device based upon if a user identity has the device associated with the specific service request. If a user has the correct service association, access is granted. If not, access is denied.

The possible set of services that can be associated with a user is:

- ***VNC* (options: Standard, Linux, Web version)**– graphical access to a device (requires a VNC Server service to be installed and running on the device)
- ***Telnet*** – standard, unsecured Telnet access to a device
- ***SSH* –** secured, in-band console access to a device (requires a SSH v1 or v2 server (daemon) to be installed and running on the device)
- ***SSH2Telnet* –** allows secured access to a Telnet-enabled device by using the secure shell protocol for communications between the client and the GateKeeper appliance, All subsequent connections from the GateKeeper appliance to the target Telnet server (deamon) will be using the plain text Telnet protocol. This methodology allows for strict enforcement of only approved encrypted protocols outside of the protected network.
- ***R DP* –** Remote desktop connection (required the remote desktop connection enabled)
- ***Out-of-Band*** – serial (RS-232) console access of a device. (requires a network enabled serial concentrator supporting reverse telnet or reverse SSH)
- ***Power*** – remote boot (power on/off/reboot) of a device. (requires a network enabled “smart power” concentrator supporting reverse telnet or reverse ssh)
- ***Service*** – Other services defined by the authorized administrator (e.g. fat client access such as SQL query frontends, Mainframe clients, or any proprietary applications which utilize TCP or UDP connections)

The TOE supports two additional access checks that layer on the device access control policy. The first access check is the socket filtering policy. This policy is implemented using an agent on the backend Windows or UNIX device. The agent on the backend device runs as a service on Windows or a daemon on UNIX. When a user successfully accesses a device, the GateKeeper device pushes a policy to the corresponding agent on the device if the socket policy is enabled. The communication between the GateKeeper and the agent is protected using SSL. The socket policy only permits an associated user to use specific sockets on the backend device. The administrator has the option of creating a white list or a black list on a per user and device pair combination. The white list permits access to only those sockets included in the list. A black list denies the specific sockets listed and permits all others. Either a white or black list can be active at one time; they are mutually exclusive.

The second access check support is a command filter. The administrator has the option of creating a white list of permitted commands or a black list of denied commands on a per device basis. The command filter is enforced on the GateKeeper appliance. The GateKeeper appliance intercepts all user traffic and performs pattern matching on all keystrokes. This enables the GateKeeper to filter specific commands on a per user and device pair combination. This filtering is possible because users must first logon to the Gateway appliance before accessing any backend device with any service. The appliance is permitted to be a man-in-the-middle in this scenario.

.

6.1.4 Identification and Authentication

FIA_ATD.1 User Attribute Definition

Authorized administrator and user accounts in the TOE have the following attributes: user name, userID, authentication data (password), and assigned privileges. The authentication data can be set to required levels using additive hierarchal strength as defined by the administrator including the following: 0-Require New Password, 0+1-Require length of X to Y as set by administrator, 1+2-Require Alpha-Numeric, 2+3-Require Upper and Lower Case, 3+4-Require Special Characters. The evaluated configuration requires level 2 to be set by the administrator and the minimum password length is six characters.. The authentication data is encrypted and stored inside the TOE. SSL is used to ensure secure access to the login interface.

A TOE administrator configures custom module permissions per user (a person configured for access to the TOE). The user entity includes both account (UserId and password) and non security relevant contact information (First name, Last Name, Phone number, Beeper number, Email address, other description such as department, location, etc) for a user. Both an administrator and a user can update the user's entity information (Password, First Name, Last Name, Phone number, Beeper number, Email address, other description such as department, location, etc.)

Module permissions (i.e., privileges) determine the features that the user will have access to, and type of user (access and/or monitor). Typically users have access and monitoring permissions, and administrators have all permissions.

FIA_UAU.2 User Authentication before Any Action, FIA_UID.2 User identification before any action, and FIA_UAU.5 Multiple Authentication mechanisms

The Identification and Authentication security function provides for user logon (authorized administrators and users), and management of user profiles.

The administrative log-in and administration configuration modules allow for Configuration and Administration of the TOE itself, as well as the permission to create/update/delete Users, Devices, and Associations. Access is restricted to an administrator. Once authenticated, the administrator creates associations between a specific User and a specific Device Associations are enforced by the TOE. This includes what devices each user is allowed to access and/or manage. The association also controls what type of access the user will have to each Device.

The TOE provides multiple authentication mechanisms. In all cases, the TOE requires users (authorized administrators and users) to provide unique identification and authentication data (UserId and passwords) before any access to the system is granted. The TOE provides a password mechanism where if the password comparison is the same between the user and TOE stored password, the user is granted access. Secondly, the TOE can use a third-party LDAP server to validate passwords. In this case, the TOE enforces the decisions it receives from the LDAP server. Lastly, the TOE can perform authentication using client certificates. No administrative or user actions are allowed until successful authentication as an authorized administrator or user.

6.1.5 Security Management

FMT_SMR.1 Security Roles

The ST identifies three roles upon which the SFRs are defined – authorized administrators, configurators, and users authorized to update their authentication data.

The TOE realizes two authorized administrator roles with pre-defined accounts, Administrator (username "super") and Configurator (username"config").. Administrators can define other users each with its own set of privileges. The Configurator is able to access configuration pages (https://TOEip/config/) to configure additional network information, monitor settings, and purge logs. When a new user account is created, it can be assigned one or more privileges. User accounts with no administrative privileges are called users. Users and Administrators are able to view/modify authentication data and contact information.

There are two pre-defined administrators in the TOE - Administrator and Configurator. Different types of administrators can be created but all users with any ability to manage TOE data are administrators in CC terminology. The TOE restricts the management of access control to authorized administrators. Only authorized administrators are able to enable, disable or modify the behavior of administrator accounts.

.

Authorized administrators control the TSF. A TOE administrator configures custom permissions per user (a person configured for access to the TOE). The TOE consists of a number of administrative modules, which is a set of button selections available at the top of the screen on the user's web browser window each with its own set of features. A user's permissions are controlled by their access to the modules. Administrative module permissions determine the features and devices that the user will have access to by limiting the features a user can access.

The user entity includes both account and contact information for a user. Both an administrator and a user can update the user's entity information with the exception of the UserId – only an administrator can create UserId.

Below is a summary of the Administration Modules:

- Sessions – a setting used to manage active logins, to view logs and view/create audit reports. This privilege is assigned to the GateKeeper administrators
- Config – a setting allowing this user to utilize the Configuration module features (setting Login, Session timeouts, Password security level, Password failure limit and Password Change interval), assigned to the TOE administrators
- Services – a setting allowing this user to utilize the Services module features which includes creating custom access methods to run either their own local clients or launch a URL , assigned to the TOE administrators
- Users – a setting allowing this user to utilize the Users module features which includes create, update and delete user account and privileges, assigned to the TOE operation administrators
- Devices – a setting allowing this user to utilize the Devices module features which includes create, update and delete devices, assigned to the TOE operation administrators
- Associations – a setting allowing this user to utilize the Associations module features which includes create, update and delete association between users and devices, manage socket policies, and manage command filters

FMT_MSA.1 Management of security attributes

The TOE enforces the Device Access Control SFP in limiting only authorized administrators the ability to create, modify, and delete device associations.

FMT_MSA.3 Static attribute initialization

The TOE provides restrictive default values to provide enforcement of the Device Access Control SFP, which can be overridden by authorized administrators when creating device associations.

FMT_SMF.1 Specification of management functions

The TOE provides the ability to manage user accounts, including the ability to create, delete and modify existing accounts, to authorized administrators.

The TOE provides an authorized administrator the ability to manage audit and log functions by providing an audit review capability in the reporting menu. The administrator is also permitted to purge the audit logs.

The TOE provides the ability for the Configurator to set the timestamp used for auditing.

The TOE permits authorized administrators to record sessions. These sessions can then be offloaded to a server configured by the authorized administrator. The recorded sessions are protected by a SHA-1 hash to ensure the integrity of the data upon review.

FMT_MTD.1(a) Management of TSF Data (Security-Relevant Privileges), FMT_MTD.1(d) Management of TSF Data (User Identity)

The TOE restricts the ability to administer the security-relevant privileges for users to only authorized administrators.

The TOE restricts the ability to assign modules to users through authorized administrators. All users must change their default authentication information when they try to access TOE first time. Users and administrator are able to update authentication information. Successful authentication provides administrators to create/modify/delete

.

services, users, devices and associations. In Create User GUI, administrators are able to define a UserId and define or modify module privileges for user. The Create User interface also provides the authorized administrator the ability to configure authentication as local. In the evaluated configuration, all authentication is local.

FMT_MTD.1(b) Management of TSF Data (Authentication Data)

The administrative module provides the abilities for only authorized administrators to create users and assign privileges. Both authorized administrators and users can change user passwords. Users can change their own passwords.

FMT_MTD.1(c) Management of TSF Data (Timestamp)

The administrative module provides the abilities for only authorized administrators to set the hardware clock supplied with the device. This function is restricted to the Configurator by default.

FMT_MTD.1(e) Management of TSF Data (Audit Data)

The administrative module provides the abilities for only authorized administrators to perform the following tasks:

To view and query the audit logs

To select audit events

To purge audit logs

FMT_MTD.1(f) Management of TSF Data (Certificate Management)

The administrative module provides the abilities for only authorized administrators to manage the x.509v3 certificates. Administrators have the ability to request certificate and key generation, upload certificates and private keys and to download of x.509v3 certificates.

6.1.6 Protection of Security Functions

FPT_FLS.1 Failure with preservation of secure state

The TOE provides clustering functionality which allows failing over in the event of a GateKeeper outage. When the user logs into the cluster address they are automatically redirected to the least-loaded cluster node. For the duration of that user's session they, and all requests, are bound to that node. If a nodes goes down it also takes down any users connected to it, but new users logging in will be redirected to one of the surviving nodes. Users who were knocked off simply need to re-connect to the cluster address.

FPT_STM.1 Reliable timestamp

The TOE includes a hardware time clock within the appliance which is used to stamp all records generated by the TOE. Optionally the TOE can use an ntp server to acquire timestamps used for audit records.

7. Protection Profile Claims

There are no PP claims for this evaluation.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;

.

- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	O.PROTECT	O.ACCESS	O.AUDIT	O.TIME	O.AUDIT_PROTECTION	O.MANAGE	O.RECOVER_STATE
T.AUDIT_COMPROMISE					X		
T.PRIVIL		X					
T.TSF_COMPROMISE		X					
T.UNAUTH_ACCESS		X					
P.MANAGE		X				X	
P.PROTECT	X	X					X
P.AUDIT			X	X			

Table 3 Environment to Objective Correspondence

8.1.1.1 T.AUDIT_COMPROMISE

A user may cause audit data to be inappropriately accessed (viewed, modified or deleted), or prevent future records from being recorded, thus masking an attacker's actions.

This threat is countered by ensuring that the TOE must provide protection for its audit data (O.AUDIT_PROTECTION).

8.1.1.2 T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.ACCESS objective ensures that users only have the appropriate access to TOE functions and data for which they are authorized.

.

8.1.1.3 T.TSF_COMPROMISE

A malicious user may cause the TOE, configuration data, or sensitive user data to be inappropriately accessed (viewed, modified or deleted) allowing a breach in the TSF security policies

The environment will protects the TSF from a compromise through physical means (OE.PHYCAL). Logically, the O.ACCESS objective ensure that users can only access TSF functions and data for which they are authorized.

8.1.1.4 T.UNAUTH_ACCESS

A user may gain unauthorized access to devices.

This Threat is countered by ensuring access to devices is controlled by a discretionary policy enforced by the TOE (O.ACCESS).

8.1.1.5 P.MANAGE

The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE.

The O.MANAGE security objective supports this policy by ensuring that the TOE provides management functions for the authorized administrators use. The O.ACCESS security objective support this objective by allowing only authorized users to access the TOE resources. The O.ACCESS supports this policy by only allowing authorized users to access only appropriate TOE functions and data as defined by the administrator.

8.1.1.6 P. PROTECT

The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

The O.ACCESS objective supports this policy by requiring authentication prior to all access to any data, only allowing authenticated and authorized users access to the TOE, and allowing permitting functions to be performed which are authorized for the user. The O.PROTECT objective addresses this policy by providing TOE self-protection. The O.RECOVER_STATE objective ensures the TOE remains secure in the event of an inoperable TOE.

8.1.1.7 P. AUDIT

Users of the system shall be accountable for their security relevant actions within the system..

The O.AUDIT objective supports this policy by requiring that all security relevant actions are recorded and can be reviewed by authorized administrators. The O.TIME objective supports this policy by providing a reliable timestamp that is used in the audit records.

8.1.1.8 Security Objectives for the Non-IT Environment Rationale

Table 4: Security objectives for the non-IT environment mapped to assumptions identifies security objectives for the non-IT environment in which the TOE is designed to operate and provides a mapping to assumptions that are made about that environment.

Security Objectives for the Non-IT Environment	Assumptions
OE.INSTALL	A.MANAGE A.CONNECT
OE.PERSON	A.NOEVIL
OE.PHYCAL	A.LOCATE

.

Table 4: Security objectives for the non-IT environment mapped to assumptions

OE.INSTALL - Ensuring proper installation, management, and operation of the TOE to protect both itself and its resources addresses the assumption A.MANAGE. Proper installation of the TOE will ensure that all network traffic passes through the TOE which addresses the A.CONNECT assumption.

OE.PERSON - This objective ensures that the TOE is operated in a secure manner by competent, non-hostile, trained personnel, which addresses A.NOEVIL assumption.

OE.PHYCAL - This objective ensures that the TOE is operated in an environment that will protect it from physical threats and attacks that can disturb and corrupt the information generated. This objective addresses A.LOCATE.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that Table 5 indicates the requirements that effectively satisfy the individual objectives.

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.PROTECT	O.ACCESS	O.AUDIT	O.AUDIT_PROTECTION	O.TIME	O.MANAGE	O.RECOVER_STATE
FAU_GEN.1			X				
FAU_SAR.1			X	X			
FAU_SAR.2			X	X			
FAU_SAR.3			X				
FAU_STG.1				X			
FCS_CKM.1	X						
FCS_CKM.4	X						
FCS_COP.1	X						
FDP_ACC.1		X					
FDP_ACF.1		X					
FIA_ATD.1		X					
FIA_UAU.2	X						
FIA_UAU.5	X						

	O.PROTECT	O.ACCESS	O.AUDIT	O.AUDIT_PROTECTION	O.TIME	O.MANAGE	O.RECOVER_STATE
FIA_UID.2	X						
FMT_MSA.1						X	
FMT_MSA.3						X	
FMT_SMF.1						X	
FMT_SMR.1	X						
FMT_MTD.1(a)	X	X				X	
FMT_MTD.1(b)	X	X		X		X	
FMT_MTD.1(c)	X	X			X	X	
FMT_MTD.1(d)	X	X				X	
FMT_MTD.1(e)	X	X				X	
FMT_MTD.1(f)	X	X				X	
FPT_FLS.1							X
FPT_ITT.1	X						
FPT_STM.1					X		

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.PROTECT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to identify and authenticate all users prior to any access and does not provide any authentication data feedback to users. [FIA_UAU.2, FIA_UID.2, FIA_UAU.5] The TOE encrypts authentication data between itself and users. [FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPT_ITT.1] The TOE requires that users be assigned to roles to determine the level of access granted to the TOE. [FMT_SMR.1, FMT_MTD.1(a),(b),(c),(d),(e)(f)].].

8.2.1.2 O.ACCESS

The TOE must allow authorized users to access only appropriate TOE functions and data as defined by the administrator.

The TOE must prevent unauthorized users from accessing the administrative modules. [FMT_MTD.1(a),(b),(c),(d),(e)(f)]. The TOE requires that all users of the TOE be unique and have unique identifiers. [FIA_ATD.1]. The unique identifiers are user to limit access to TOE functions [FDP_ACF.1].

8.2.1.3 O.AUDIT

The TOE must record the security relevant actions of users of the TOE and must present this information in a readable format to authorized administrators.

.

The TOE will record security relevant events that include details about the events themselves in an audit trail that can be reviewed only by authorized administrators. [FAU_GEN.1, FAU_SAR.1, FAU_SAR.2]. The TOE permits the authorized administrator the ability to search the audit trail based upon all the data in the audit trail [FAU_SAR.3]

8.2.1.4 O.AUDIT_PROTECTION

The TOE must provide the capability to protect audit information.

The TOE prevents unauthorized deletion or modification of audit records [FAU_STG.1]. The TOE only permits the authorized administrator to access the audit trail [FAU_SAR.2].

8.2.1.5 O.TIME

The TOE must provide reliable time stamps for audit records.

The TSF shall be able to provide reliable time stamps for its own use [FPT_STM.1.1]. The TSF restricts access to the timestamp to the configurator [FMT_MTD.1c].

8.2.1.6 O.MANAGE

The TOE must provide services that allow effective management of its functions and data.

The TOE must provide the authorized administrators the ability to manage the user accounts of the TOE, authentication data, the timestamp, privilege assignments, certificate management, and audit data including event selection, and user identities. [FMT_MTD.1(a),(b),(c),(d),(e)(f)] The TOE places restrictions on access to the Administrative module. These restrictions include manipulating device associations,. [FMT_MSA.1, FMT_SMF.1] The TOE ensures restrictive default settings for device associations. [FMT_MSA.3].

8.2.1.7 O.RECOVER_STATE

The TOE must provide the ability to maintain a secure state in the case the TOE becomes inoperable.

In clustering mode, the TOE provides the ability for one GateKeeper to rollover to a functional GateKeeper if the machine becomes inoperable.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL4 augmented with ALC_FLR.2 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a moderate level of risk to the assets. The security environment assumes physical protection and the TOE itself offers only a very limited interface and can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. As such, it is believed that EAL4 augmented with ALC_FLR.2 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 6 Requirement Dependency Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES

.

Functional Component	Dependency	Included
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_STG.1	FAU_GEN.1	YES
FCS_CKM.1	FCS_CKM.4, FCS_COP.1	YES
FCS_CKM.4	FCS_CKM.1, FCS_COP.1	YES
FCS_COP.1	FCS_CKM.1, FCS_CKM.4	YES
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1	YES
FIA_UAU.2	FIA_UID.1	YES (FIA_UID.2)
FIA_UAU.5	None	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	YES (FDP_ACC.1)
	FMT_SMR.1	YES
	FMT_SMF.1	YES
FMT_MSA.3	FMT_MSA.1	YES
	FMT_SMR.1	YES
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	YES (FIA_UID.2)
FMT_MTD.1(a)(,b),(c),(d),(e),(f)	FMT_SMF.1	YES
	FMT_SMR.1	YES
FPT_FLS.1	None	
FPT_ITT.1	None	
FPT_STM.1	None	

Table 6 Requirement Dependency Rationales

8.5 Extended Requirements Rationale

There are no extended requirements.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

.

	AUDITING	CRYPTOGRAPHIC SUPPORT	ACCESS CONTROL	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	SELF PROTECTION
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FCS_CKM.1		X				
FCS_CKM.4		X				
FCS_COP.1		X				
FDP_ACC.1			X			
FDP_ACF.1			X			
FIA_ATD.1				X		
FIA_UAU.2				X		
FIA_UAU.5				X		
FIA_UID.2				X		
FMT_MSA.1					X	
FMT_MSA.3					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FMT_MTD.1(a)					X	
FMT_MTD.1(b)					X	
FMT_MTD.1(c)					X	
FMT_MTD.1(d)					X	
FMT_MTD.1(e)					X	
FMT_MTD.1(f)					X	
FPT_FLS.1						X
FPT_ITT.1		X				
FPT_STM.1						X

Table 7 Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See section 7, Protection Profile Claims.

.