


PGP Corporation [®] Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6

Security Target

Evaluation Assurance Level: 2
Document Version: 0.6

Prepared for:	Prepared by:
	
PGP Corporation 200 Jefferson Drive Menlo Park, CA 94025 Phone: (650) 319-9000 Fax: (650) 319-9001 http://www.pgp.com	Corsec Security, Inc. 10340 Democracy Lane, Suite 201 Fairfax, VA 22030 Phone: (703) 267-6050 Fax: (703) 267-6810 http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2008-02-15	Greg Milliken	Initial draft.
0.2	2008-04-21	Greg Milliken	Addressed verdict OR #1
0.3	2008-06-09	Greg Milliken	Added key sizes for RSA. Removed Gateway virus scanning from the excluded functionality list (no longer supported). Updated address information. Added FMT_MSA.1(b) for cryptography dependency.
0.4	2008-10-01	Amy Nicewick	Removed FAU_STG.1 and added environmental objective; changed name of TOE; added OS to TOE description; added guidance document names.
0.5	2008-10-09	Amy Nicewick	Addressed CB OR #1.
0.6	2008-10-20	Amy Nicewick	Added FIPS certificate number.

Table of Contents

REVISION HISTORY	2
TABLE OF CONTENTS	3
TABLE OF FIGURES	4
TABLE OF TABLES	4
1 SECURITY TARGET INTRODUCTION	6
1.1 PURPOSE.....	6
1.2 SECURITY TARGET AND TOE REFERENCES	7
1.3 TOE OVERVIEW	7
1.3.1 <i>Universal Server Concepts</i>	9
1.3.2 <i>TOE Environment</i>	12
1.4 TOE DESCRIPTION	12
1.4.1 <i>Physical Scope</i>	13
1.4.2 <i>Logical Scope</i>	14
1.4.3 <i>Modes of Operation</i>	16
1.4.4 <i>Excluded Functionality</i>	16
2 CONFORMANCE CLAIMS.....	17
3 SECURITY PROBLEM DEFINITION	18
3.1 THREATS TO SECURITY.....	18
3.2 ORGANIZATIONAL SECURITY POLICIES	19
3.3 ASSUMPTIONS	19
4 SECURITY OBJECTIVES	21
4.1 SECURITY OBJECTIVES FOR THE TOE.....	21
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	22
4.2.1 <i>Information Technology (IT) Security Objectives</i>	22
4.2.2 <i>Non-IT Security Objectives</i>	22
5 EXTENDED COMPONENTS DEFINITION	24
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS	24
5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS	25
6 SECURITY REQUIREMENTS.....	26
6.1 CONVENTIONS	26
6.2 SECURITY FUNCTIONAL REQUIREMENTS	26
6.2.1 <i>Class FAU: Security Audit</i>	28
6.2.2 <i>Class FCS: Cryptographic Support</i>	29
6.2.3 <i>Class FDP: User Data Protection</i>	32
6.2.4 <i>Class FIA: Identification and Authentication</i>	35
6.2.5 <i>Class FMT: Security Management</i>	38
6.2.6 <i>Class FPT: Protection of the TOE Security Function</i>	41
6.2.7 <i>Class FTA: TOE Access</i>	41
6.3 SECURITY ASSURANCE REQUIREMENTS	42
6.4 TOE SECURITY ASSURANCE MEASURES	42
6.4.1 <i>ALC_CMC.2: Use of a CM system, ALC_CMS.2: Parts of the TOE CM coverage</i>	44
6.4.2 <i>ALC_DEL.1: Delivery Procedures</i>	44
6.4.3 <i>ADV_ARC.1: Security Architecture Description, ADV_FSP.2: Security-enforcing Functional Specification, ADV_TDS.1: Basic design</i>	44
6.4.4 <i>AGD_OPE.1: Operational User Guidance, AGD_PRE.1: Preparative Procedures</i>	44
6.4.5 <i>ATE_COV.1: Evidence of Coverage, ATE_FUN.1: Functional Testing</i>	45
7 TOE SUMMARY SPECIFICATION.....	46

7.1	TOE SECURITY FUNCTIONS.....	46
7.1.1	Security Audit.....	47
7.1.2	Cryptographic Support.....	48
7.1.3	User Data Protection.....	49
7.1.4	Identification and Authentication.....	49
7.1.5	Security Management.....	50
7.1.6	Protection of the TSF.....	50
7.1.7	TOE Access.....	51
8	RATIONALE.....	52
8.1	CONFORMANCE CLAIMS RATIONALE.....	52
8.2	SECURITY OBJECTIVES RATIONALE.....	52
8.2.1	Security Objectives Rationale Relating to Threats.....	52
8.2.2	Security Objectives Rationale Relating to Policies.....	55
8.2.3	Security Objectives Rationale Relating to Assumptions.....	55
8.3	RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS.....	58
8.4	RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS.....	58
8.5	SECURITY REQUIREMENTS RATIONALE.....	58
8.5.1	Rationale for Security Functional Requirements of the TOE Objectives.....	58
8.5.2	Security Assurance Requirements Rationale.....	62
8.5.3	Dependency Rationale.....	62
9	ACRONYMS AND TERMINOLOGY.....	65
9.1	ACRONYMS.....	65
9.2	TERMINOLOGY.....	66

Table of Figures

FIGURE 1 – GATEWAY PLACEMENT DEPLOYMENT CONFIGURATION OF THE TOE.....	8
FIGURE 2 – INTERNAL PLACEMENT DEPLOYMENT CONFIGURATION OF THE TOE.....	8
FIGURE 3 – IGNITION SECRET.....	11
FIGURE 4 – PHYSICAL TOE BOUNDARY.....	13

Table of Tables

TABLE 1 – SECURITY TARGET (ST) AND TARGET OF EVALUATION (TOE) REFERENCES.....	7
TABLE 2 – COMMON CRITERIA (CC) AND PROTECTION PROFILE (PP) CONFORMANCE.....	17
TABLE 3 – THREATS.....	18
TABLE 4 – ASSUMPTIONS.....	19
TABLE 5 – SECURITY OBJECTIVES FOR THE TOE.....	21
TABLE 6 – IT SECURITY OBJECTIVES.....	22
TABLE 7 – NON-IT SECURITY OBJECTIVES.....	22
TABLE 8 – TOE SECURITY FUNCTIONAL REQUIREMENTS.....	26
TABLE 9 – CRYPTOGRAPHIC KEY GENERATION STANDARDS.....	29
TABLE 10 – CRYPTOGRAPHIC OPERATIONS.....	30
TABLE 11 – MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR.....	38
TABLE 12 – ASSURANCE REQUIREMENTS.....	42
TABLE 13 – ASSURANCE MEASURES MAPPING TO TOE SECURITY ASSURANCE REQUIREMENTS (SARS).....	43
TABLE 14 – MAPPING OF TOE SECURITY FUNCTIONAL REQUIREMENTS TO SECURITY FUNCTIONAL REQUIREMENTS.....	46
TABLE 15 – THREATS:OBJECTIVES MAPPING.....	52
TABLE 16 – ASSUMPTIONS:OBJECTIVES MAPPING.....	55
TABLE 17 – OBJECTIVES: SECURITY FUNCTIONAL REQUIREMENTS (SFRs) MAPPING.....	58

TABLE 18 – FUNCTIONAL REQUIREMENTS DEPENDENCIES 62
TABLE 19 – ACRONYMS 65
TABLE 20 – TERMINOLOGY 66

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6, and will hereafter be referred to as the TOE or Universal Server throughout this document. The TOE is a software application that serves as an email proxy and encryption gateway. The TOE provides secure messaging with little or no user interaction. The TOE automatically creates and maintains a security architecture by monitoring authenticated users and their email traffic. Users can also send protected messages to addresses that are not part of the security architecture.

1.1 Purpose

This ST provides mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats in the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims.
- Security Problem Definition (Section 3) – Describes the threats, policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 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 (Section 6) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terminology (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – Security Target (ST) and Target Of Evaluation (TOE) References

ST Title	PGP Corporation ® Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 Security Target
ST Version	Version 0.6
ST Author	Corsec Security, Inc. Greg Milliken and Amy Nicewick
ST Publication Date	October 20, 2008
TOE Reference	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6
Keywords	PGP, Email Gateway, Universal Server, Public Key Encryption, Email Encryption, Transparent Encryption

1.3 TOE Overview

The PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 is a proprietary software application designed to act as an email proxy. The purpose of the application is to provide encryption and signing services for email messages entering or leaving the local network. Universal Server transparently encrypts or decrypts messages using a user's public key. If a user does not have a PGP key pair, Universal Server automatically generates one for the user. Universal Server manages a list of public keys for internal users and allows both internal and external users to access a list of public keys for internal users.

The TOE can be placed onto the network in one of two different base configurations: Gateway Placement and Internal Placement. In Gateway Placement, the TOE sits between the mail server and the external network. Email messages are sent and received over Simple Mail Transfer Protocol (SMTP), and are secured before they are sent to the Internet (on the way to their destination) and decrypted and verified when received from the Internet .

In Internal Placement, the TOE sits between email users and their email server. With an Internal Placement of the TOE, messages are secured based on applicable policies when they are sent to the mail server using SMTP. Messages are decrypted and verified when they are retrieved from the mail server using Post Office Protocol or Internet Message Access Protocol.

Figure 1 shows the details of the Gateway Placement deployment configuration of the TOE:

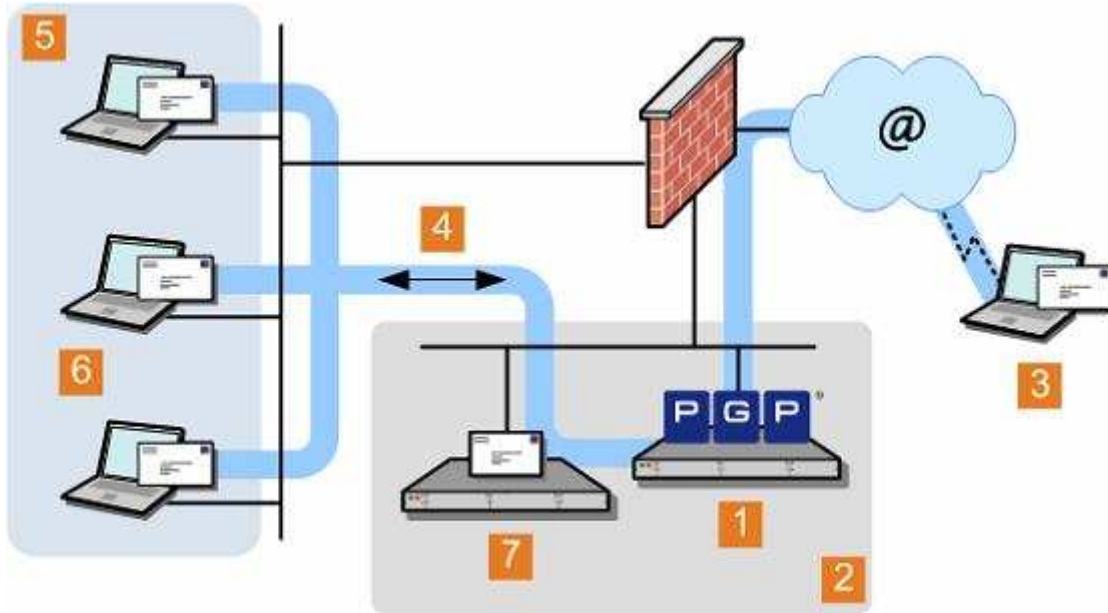


Figure 1 – Gateway Placement Deployment Configuration of the TOE

- 1) PGP Universal Server Gateway Placement
- 2) De-Militarized Zone
- 3) External email user
- 4) Logical flow of data
- 5) Internal network
- 6) Email users
- 7) Email server

Figure 2 shows the details of the Internal Placement deployment configuration of the TOE:

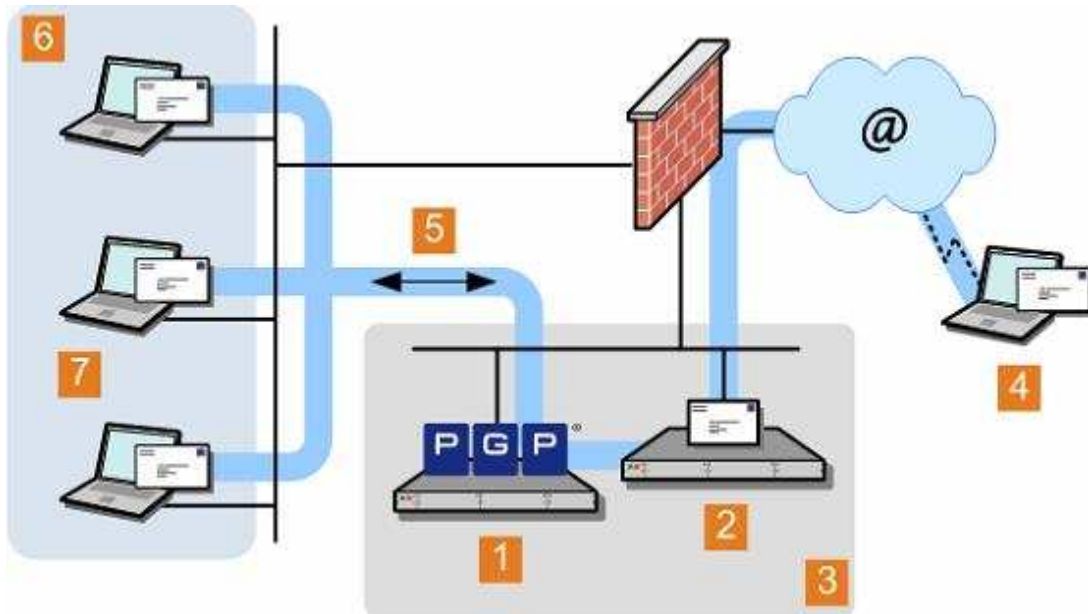


Figure 2 – Internal Placement Deployment Configuration of the TOE

- 1) PGP Universal Server
- 2) Email server
- 3) De-Militarized Zone
- 4) External email user
- 5) Logical flow of data
- 6) Internal network
- 7) Email users

In addition to the two base configurations, there are several advanced placement configurations. Examples of advanced configurations include clustered, load balanced, and large corporation configurations. For a detailed description of these configurations, please refer to the *PGP Universal Server Administrator's Guide*.

Universal Server can provide the following security services:

- apply public key cryptographic operations on email traffic originating from the internal or external network
- control the flow of email messages into and outside of the internal network
- manage the entire key lifecycle for internal users including key generation and key destruction

Control is achieved by enforcing a configurable policy (Email Security Functional Policy (SFP)) on email traffic flowing to and from the email users. The policy may be based on message contents, attachments, user or group permissions, and a variety of other factors listed in section 6. In addition, Universal Server provides management of public and private keys for email users and access to email users' public keys.

1.3.1 Universal Server Concepts

This section presents the key concepts necessary to understanding the way the Universal Server functions.

1.3.1.1 Security Architecture

Universal Server automatically creates and maintains a security architecture for the users whose email domain it is securing. Since Universal Server automatically maintains the security architecture, the security architecture is a Self-Managing Security Architecture (SMSA). SMSA refers to all the ways Universal Server helps keep data secure.

1.3.1.2 Learn Mode

When the Universal Server is first installed and turned on, it operates in Learn Mode. While in Learn Mode, the Universal Server does not encrypt or sign any messages, but proxies traffic and decrypts and verifies incoming email.

Learn Mode allows the Universal Server to build the SMSA. When an administrator disables Learn Mode the Universal Server knows the environment and can begin securing email messages.

Administrators can examine the effects of policies on email traffic while the product is operating in Learn Mode. Any adverse effects resulting from misapplied policies do not affect email traffic. Administrators examine policy effects by viewing the System Log, which records what the Universal Server would be doing if Learn Mode were disabled.

1.3.1.3 Administrative Interface and Multiple Administrators

Universal Server is controlled via a web-based Administrative Interface. The initial setup of the TOE is performed through the setup assistant portion of the Administrative Interface, which loads automatically the first time an administrator logs in. After the initial configuration is complete, the server automatically restarts and administrators can log in via the Administrative Interface and configure all settings for the Universal Server.

There are six levels of administrator access, each with a pre-defined set of permissions. Roles range from SuperUser, which can modify all configuration settings and perform all administrative tasks, to Read-only Administrator, which can only view settings and the System Log. Multiple administrators can be logged onto the Universal Server simultaneously. Race conditions are handled either by allowing the last administrator to submit a setting to “win”, or by giving the administrators an error if the setting is sensitive to simultaneous modifications.

1.3.1.4 Email Policy

The main function of the Universal Server is the ability to process email messages based on a set of policies. Administrators configure Universal Server with appropriate policies through the Administrative Interface. The policies can apply to inbound and outbound messages. Administrators configure policy through multiple policy chains that are comprised of sets of rules. The rules in the chains govern the behavior of the Universal Server while processing a given policy chain. Each policy chain processes different kinds of email. Chaining multiple policy chains together allows for granular control of email traffic flowing through the Universal Server.

Policy chains consist of rules, which are sets of conditions and actions. Universal Server applies rules to messages in sequential order. If a message meets the conditions for a rule, the rule takes effect. If the message does not meet any conditions, the Universal Server goes on to the next rule in the chain.

For mail policies to be applied to messages from internal users to other internal users, the Universal Server must be configured with the Internal Placement Deployment Configuration.

Dictionaries are lists of terms to be matched in policy definitions. The dictionaries work with mail policy to allow administrators to define content lists that can trigger rules. Universal Server dictionaries contain addresses that should be excluded from processing, key words (e.g. “confidential”, “iloveyou”), and user names for internal users whose messages require special handling.

A rule in a policy chain can have a condition that checks certain parts of the message against a dictionary. If the relevant part of the message contains a term that matches a term in the dictionary, the rule is triggered and the action is carried out. Dictionaries can be maintained without being used in any rules.

1.3.1.5 Clustering

A cluster is when two or more Universal Servers are on the same network and configured to synchronize with each other. In a cluster, one server is always designated Primary, while the other servers are Secondary. Secondary servers synchronize their users, keys, managed domains, and policies with the Primary server.

When a Secondary server becomes unavailable and disconnects from the Primary server, the Secondary server stops receiving synchronized data. A Secondary server resynchronizes with the Primary server if the Secondary server is disconnected for more than 24 hours. If the Secondary server is disconnected for less than 24 hours, then the synchronization data is queued up and sent to the Secondary server without need for a lengthy resynchronization. When the Primary server fails, no other server assumes the Primary role. The Secondary servers are capable of carrying out the functions of the Universal Server without a Primary server for the duration that the Primary server is disconnected. Synchronization data is protected with Transport Layer Security (TLS).

Clustering allows lower overhead (since the load on the system is spread between the different servers in the cluster). Clustering also allows redundancy, because if one server fails (including the Primary server), the other servers continue processing messages.

1.3.1.6 Organization Key and Certificate and Ignition Key and Secret

The Organization Key is a key pair Universal Server uses to sign all user keys that the Universal Server manages. Universal Server also uses the Organization Key when encrypting backups. The Organization Key is generated by the Setup Assistant during the initial configuration of the Universal Server. The Organization Key renews itself with the same settings the day before it is due to expire.

The Organization Certificate is an X.509 certificate that can either be self-signed or requested from a Certificate Authority (CA). The Universal Server uses the Organization Certificate to generate X.509 certificates for internal users and to provide Secure Multipurpose Internet Mail Extensions functionality. If users already have an X.509 certificate associated with their keys, the users do not receive a new certificate until the old certificate expires.

The TOE can be configured to require one or more Ignition Key to boot. The Ignition Keys are ordinary PGP key pairs. The Ignition keys can be either hardware and software (requiring a USB key and a passphrase), or it can be software-only (requiring only a passphrase to boot).

The Ignition Secret and Ignition Key go hand in hand in preventing catastrophic data loss in the event that an intruder gains physical access to the Universal Server. The Ignition Secret itself is a randomly generated Advanced Encryption Standard (AES) key. This AES key is used to encrypt sensitive information on the box, such as users' private keys, Web Messenger message texts, etc.

The Universal Server needs to protect this AES key. Universal Server needs to record the AES key onto non-volatile memory because Universal Server needs to survive reboots and the like. The private parts of the Ignition Keys are encrypted to secrets that only the administrators know (either passphrases or physical token material). The Ignition Keys are then used to create encrypted copies of the Ignition Secret, and those encrypted copies are then stored on disk.

In order to "unlock" the Universal Server and begin the bootstrap process, (i.e. to get at the Ignition Secret's unencrypted key material), an administrator needs to provide the passphrase or token that encrypts any one of the Ignition Keys. The Ignition Key's private key is then used to decrypt the Ignition Secret, and the Ignition Secret is used to decrypt the sensitive material that it is protecting on the Universal Server.

The following diagram shows these relationships graphically:

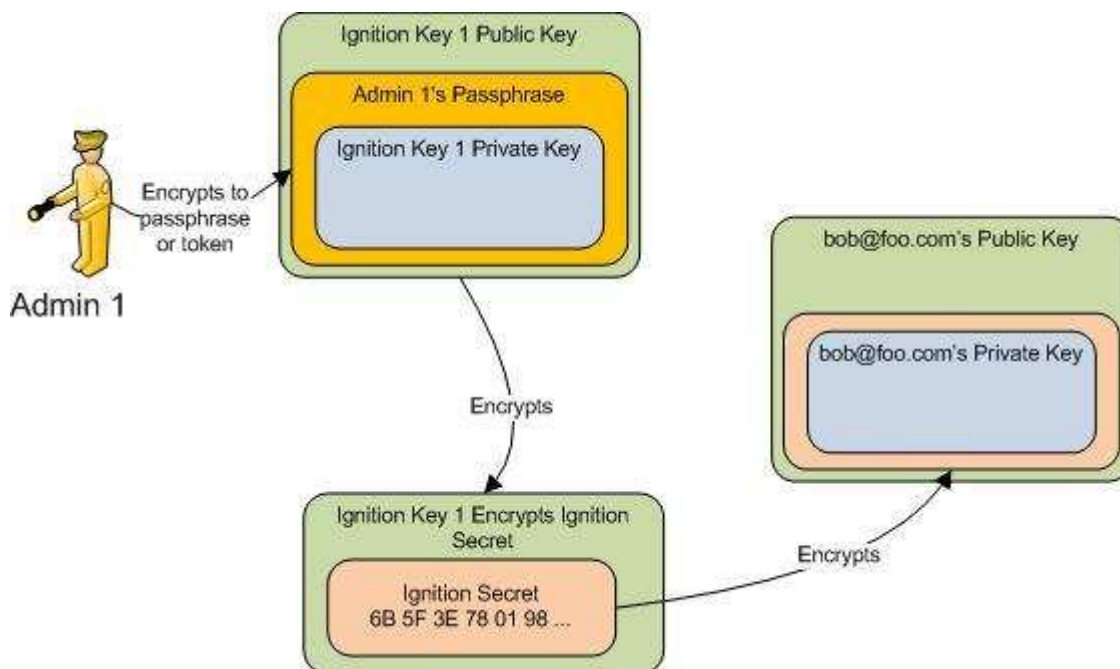


Figure 3 – Ignition Secret

The Ignition Key's passphrase that an administrator knows is not necessarily the same as that administrator's login passphrase. The two passphrases can be the same or totally different, depending on the administrator and the company's policy.

1.3.1.7 Additional Features

The Universal Server supports integration of Lightweight Directory Access Protocol (LDAP) directories. LDAP traffic is secured with TLS when configured. With Directory Synchronization, administrators can define user policies for specific internal user groups. Administrators can specify users from the directory to include or exclude, and users to which user policies will be applied. When Universal Server imports users from an LDAP directory, the server imports the user's names, email addresses, and any existing X.509 certificates. Unsupported or weak certificates are not imported, nor are certificates with email addresses from an external domain.

File Blocking allows the Universal Server to block attachments that match filenames an administrator specifies. File Blocking must be implemented through policies that specify the "bounce" or "drop" actions to be applied to the unwanted messages. The File Blocking feature cannot be used to block files based on their contents, only their file name or file type.

Verified Directory is a public-facing web service whereby users can connect to the Universal Server and submit or remove public keys, or search for other users' public keys. To help ensure the validity of keys submitted to Verified Directory, the Universal Server sends verification emails to the users who submit keys. If the key owner responds to the verification message with permission to add the key, then Universal Server allows the key to be added to the directory. Similarly, when a user removes a public key, Universal Server sends a verification email to that user making sure they intended to remove their key.

When a key listed in the Verified Directory expires, Universal Server sends a renewal email to the user who submitted the key. If the user does not respond to the renewal email, the key is removed, thereby removing the clutter of invalid and unused keys.

Universal Server provides the Web Messenger service for external recipients who do not possess the expertise or means to decrypt encrypted messages. External users receive a message from Universal Server with a link to the Web Messenger. The external user logs into Web Messenger using an account set up with the external user's email address for confirmation. The original message sent to the user is stored on Web Messenger in a protected format and the user must log in to view the message. From Web Messenger, the external user can reply to the original sender, any internal user whose credentials are stored in the Universal Server, or any of the external addresses carbon copied on the original message.

1.3.2 TOE Environment

The TOE is intended to be deployed on a supported hardware platform in a physically secured cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE provides security for email entering or leaving the Internal Network, and is meant to control, protect, and monitor email messages traveling through the TOE. For the TOE to operate correctly, all controlled email messages must traverse the TOE, and the TOE must be connected to a mail server within the logical flow of email data. The TOE environment is required to provide for this configuration.

Occasionally, when receiving a message from an external user, the TOE does not have the user's public key. In this case the TOE can be configured to look for the user's key in an external keyserver, such as the one run by PGP. The external keyserver is an optional component provided by the environment. Traffic exchanged with keyserver is protected by TLS.

The TOE can be configured to import users from an LDAP directory in a process called Directory Synchronization. For Directory Synchronization to work, the TOE must be able to connect to an LDAP server. The LDAP server is an optional component provided by the environment.

1.4 TOE Description

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

1.4.1 Physical Scope

Figure 4 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. The TOE is a software-only TOE.

The TOE is an application email proxy server bundled with the Fedora Core 6 operating system. The TOE is installed on a supported hardware platform as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are

- General purpose hardware used to store and run the TOE
- Mail server
- Mail clients

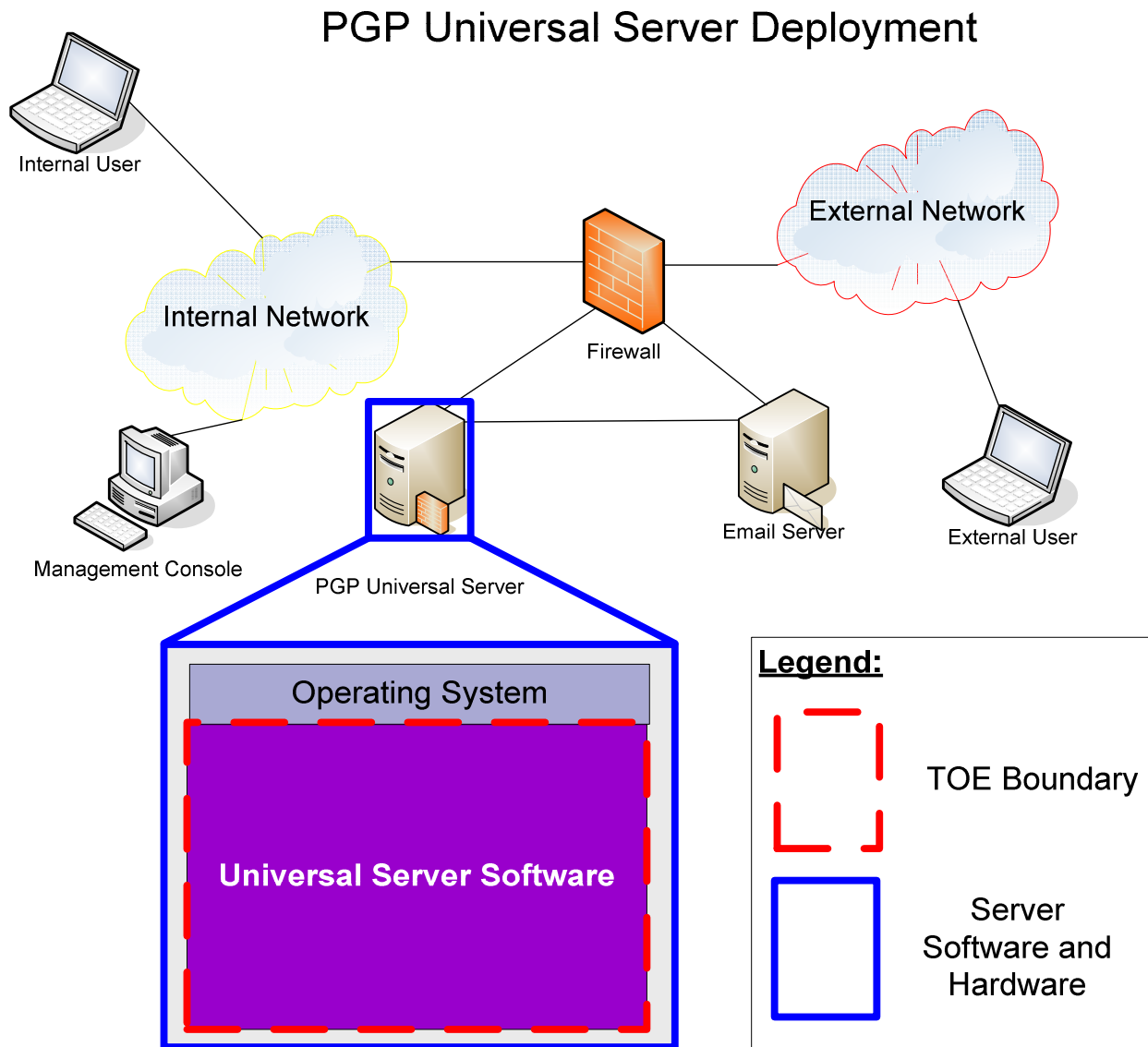


Figure 4 – Physical TOE Boundary

1.4.1.1 TOE Environment Hardware Platform

The TOE is an application email proxy server bundled with its own operating system. PGP supports running the TOE on the following hardware platforms:

- Dell PowerEdge 740
- Dell PowerEdge 860
- Dell PowerEdge 1950
- Dell PowerEdge 2950
- IBM System x346
- IBM System x3650
- IBM BladeCenter HS20 Type 7981
- Sunfire 4100
- HP Proliant BL25P
- NEC Express5800 120Ri-2
- VMWare ESX + VMtools 3.0.1
- HP Proliant DL 385 G2 w/ P400 RAID
- HP Proliant DL385 w/ P600 RAID
- HP Proliant DL385 w/ P800 RAID

The TOE testing platform is the Dell PowerEdge 860 with Dual Core Xeon 3060 processor, 1 GB RAM¹, DVD²-ROM³, and 80GB SATA⁴ hard disk drive.

1.4.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- *PGP Universal Server Administrator's Guide*
- *PGP Universal Server Version 2.9 Release Notes*
- *PGP Universal Server 2.9 Upgrade Guide*
- *PGP Universal Server 2.9 Common Criteria Supplemental*

1.4.1.3 Third-party Software

The following third-party software products are included in the TOE boundary:

- PostGRE 8.1.9 database
- Apache Tomcat Web Server 5.5.23

1.4.2 Logical Scope

The logical boundary includes the security and management engines of the Universal Server that address the security functional requirements imposed on the TOE. The security functional requirements implemented by the TOE are grouped under the following Security Function Classes:

¹ RAM – Random Access Memory

² DVD – Digital Versatile Disc

³ ROM – Read-Only Memory

⁴ SATA – Serial Advanced Technology Attachment

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Function (TSF)
- TOE Access

1.4.2.1 Security Audit

The Universal Server keeps track of auditable events through the System Log. The System Log records all auditable events in a human-readable format. Administrators can sort audit logs by type and order them by date and time. The Universal Server allows administrators to designate a Syslog server for storing backup copies of the audit logs.

1.4.2.2 Cryptographic Support

The Cryptographic Support function provides encryption and decryption of all data transmitted between the TOE and the client accessing one of the web interfaces. The TOE uses X.509 certificates for a number of purposes, including authenticating the identity of a user. The TOE can be configured to generate private keys for email users. Backup files holding sensitive data (such as private keys) are encrypted using an administrator-configured encryption algorithm. Cryptographic operations are performed by a Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module, certificate #1049.

1.4.2.3 User Data Protection

User data protection defines how users of the TOE or external Information Technology (IT) entities are allowed to perform operations on objects.

The TOE provides authorized administrators with the ability to define security policies using the Administrative Interface. The Administrative Interface provides for the creation of rules that define certain actions the Universal Server is to take based on a set of conditions. The conditions and actions affect either the flow of email traffic through the TOE (Email SFP) or the way users interact with the TOE (Web Access SFP).

1.4.2.4 Identification and Authentication

The TOE provides the ability for administrators to manage the security functions of the TOE and email users to access TOE functionality. The identification and authentication security function ensures that access to management and Web Messenger functionality is restricted to authorized TOE users and access is protected by the entry of credentials. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage. The TOE enforces a minimum quality for acceptable passphrases.

1.4.2.5 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store and access its IT assets. Administrators can use the Administrative Interface to create rules that grant and govern administrative access and rules that control the flow of email traffic.

1.4.2.6 Protection of the TSF

The TOE provides reliable timestamp information for its own use. The TOE software retrieves the timestamp from the hardware clock, which is set during installation of the appliance. The order of the audit records can be determined by the value of the timestamps.

Administrators must set the time manually through the configuration settings. Administrators are assumed to be trusted and competent, and may change the system time whenever necessary.

1.4.2.7 TOE Access

The TOE terminates a user session after a period of fifteen minutes of inactivity. Each time an action is completed by the administrator or user, the inactivity-timeout value is updated. If the time since the last activity time exceeds the inactivity timeout value, the user is logged out.

1.4.3 Modes of Operation

The TOE has two modes of operation: Learn Mode and Normal Mode. When the TOE is first installed and configured it is running in Learn Mode. Learn Mode is described in section 1.3.1.2. Normal Mode is activated when Learn Mode is disabled. Normal Mode allows the TOE to perform the full range of its functions.

1.4.3.1 Key Modes

There are four Key Modes of Operation: Server Key Mode (SKM), Client Key Mode (CKM), Guarded Key Mode (GKM) and Server-Client Key Mode (SCKM).

In SKM, the key pair, both private and public keys, are generated by the server entirely. No passphrase is set on this key when it is held by the server. The client (PGP Desktop⁵) may request a copy of the key for cryptographic operations after validating itself to the server.

In CKM, the key pair is generated by the client entirely. The client sends a copy of the public key only to the server.

In GKM, the key pair is generated by the client entirely. The client prompts the user for a passphrase for the key. The client sends the public key and passphrase-protected private key to the server. The server can't do any cryptographic operations with the passphrase protected private key, as it does not have the user's passphrase.

In SCKM, the key pair is generated on the client, and has separate encryption and signing key pairs. The client prompts the user for a passphrase for the key. The client then sends the public key and *unprotected* private key for the encryption key, and the public key and *passphrase-protected* private key of the signing key to the server. The server is able to perform decryption and encryption operations on behalf of the user, but is unable to sign messages.

1.4.4 Excluded Functionality

Features and functionality that are not part of the evaluated configuration of the TOE are:

- Key Reconstruction Blocks

⁵ PGP Desktop is a separate product developed by PGP. PGP Desktop and its functionality are not included in this evaluation.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and Protection Profile (PP) conformance claims can be found in Section 8.1.

Table 2 – Common Criteria (CC) and Protection Profile (PP) Conformance

Common Criteria CC Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of 11/19/2007 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 2 conformant

3 Security Problem Definition

This section describes the security aspects of the environment in which the TOE is 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 the TOE
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 – Security Objectives.

The following threats are applicable:

Table 3 – Threats

Name	Description
T.MASQUERADE	An attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.OPENRELAY	An attacker who is not a TOE user may send multiple SMTP messages to the TOE, whose email addresses fall outside the set of addresses for which the TOE applies policies. The intent of this attack is to utilize the resources of the TOE to deliver bulk email on behalf of the originator.
T.AUDFUL	An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.
T.USRDATA	An attacker who is not a TOE user could access individual email messages stored on the TOE, by viewing, sorting, or deleting the emails stored on the TOE.

Name	Description
T.REMCONN	An attacker who is not a TOE user may exploit network protocol(s) based vulnerabilities and compromise TOE services and data assets by establishing a remote connection to the TOE.
T.NACCESS	An attacker may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.
T.NMODIFY	An attacker may modify data that is transmitted between the TOE and a remote authorized external entity.
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for it.
T.IA	An attacker may attempt to compromise the TOE by attempting actions that the attacker is not authorized to perform on the TOE.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this Security Target.

3.3 Assumptions

This section 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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 – Assumptions

Name	Description
A.INSTALL	The TOE is installed and configured on the appropriate hardware according to the appropriate installation guides.
A.MANAGE	There are one or more competent administrators assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.FIREWALL	All ports needed for proper operation of the TOE will be opened at the firewall.

Name	Description
A.DNS	DNS information received by the TOE is reliable.
A.DIRECT	The TOE and the hardware it runs on are physically available to authorized administrators only.
A.SINGEN	Email messages cannot pass between the internal and external networks without passing through the TOE.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to provide secure email proxy functions.
A.PROTCT	The TOE shall be protected from disruptions of TOE data and functions.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 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 section identifies the security objectives for the TOE and its supporting environment. A mapping of the objectives to the threats, OSPs, and assumptions included in the security problem definition can be found in section 8.2. This mapping also provides rationale for how the threats, OSPs, and assumptions are effectively and fully addressed by the security objectives.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 5 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication ⁶ .
O.MAILRVW	The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.
O.MESACC	The TOE shall enforce an access control policy on TOE users who wish to access SMTP emails stored within the TOE.
O.PKI_CRYPTO	The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.
O.TIMESTAMP	The TOE must provide reliable timestamps for its own use.
O.LOG	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.

⁶ For a list of interfaces which do not require authentication, please see FIA_UAU.1.

4.2 Security Objectives for the Operational Environment

4.2.1 Information Technology (IT) Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 6 – IT Security Objectives

Name	Description
OE.FIREWALL	The Firewall must have all ports needed for proper operations of the TOE opened.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.TRUSTED_INFO	Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.AUDIT_STORAGE	The IT Environment will provide a means for secure storage of the TOE audit log files.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they do not require the implementation of functions in the TOE software. Thus, they are satisfied largely through the application of procedural or administrative measures.

Table 7 – Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely, including management of the audit trail.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

Name	Description
OE.AUDIT	Authorized managers of the audit facilities must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.
OE.REVIEW	The configuration of the TOE will be inspected on a regular basis to ensure that the configuration continues to meet the organization's security policies in the face of: <ul data-bbox="613 575 1438 726" style="list-style-type: none">• Changes to the TOE configuration• Changes in the security objectives of the organization• Changes in the threats presented by the hostile network• Changes (additions and deletions) in the services available between the hostile network and the corporate network
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

5 Extended Components Definition

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended SFRs defined for this Security Target.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this Security Target.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target 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 Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSP Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using “EXT_” at the beginning of the short name.

Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 8 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FCS_CKM.1	Cryptographic Key Generation		✓	✓	
FCS_CKM.3	Cryptographic Key Access		✓		
FCS_CKM.4	Cryptographic Key Destruction		✓		
FCS_COP.1	Cryptographic Operation		✓	✓	
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	

Name	Description	S	A	R	I
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓	✓	
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_SOS.1	TSF generation of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1(a)	Management of security attributes	✓	✓		
FMT_MSA.1(b)	Management of security attributes	✓	✓		
FMT_MSA.2	Secure security attributes				
FMT_MSA.3(a)	Static attribute initialization	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialization	✓	✓		✓
FMT_REV.1	Revocation	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable time stamps				
FTA_SSL.3	TSF-initiated termination		✓		

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

6.2.1 Class FAU: 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:

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [*No other auditable events*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*No other information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*administrators*] with the capability to read [*all audit information from the System Log*] 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

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*key generation type* – see **table below**] and specified cryptographic key sizes [*cryptographic key sizes* – see **table below**] that meet the following: [*list of standards* – see **table below**].

Table 9 – Cryptographic Key Generation Standards

Key Generation Method	Cryptographic Key Size	Standards
X9.31	Up to 4096 bits	X9.31 (cert #238)

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.3 Cryptographic key access

Hierarchical to: No other components.

FCS_CKM.3.1

The TSF shall perform [*cryptographic key backup*] in accordance with a specified cryptographic key access method [*symmetric encryption of backup file*] that meets the following: [*Triple-DES⁷ (FIPS 46-3 cert #471), AES-256 (FIPS 197 cert #453)*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

⁷ DES – Digital Encryption Standard

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations – see table below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see table below*] and cryptographic key sizes [*cryptographic key sizes – see table below*] that meet the following: [*list of standards – see table below*].

Table 10 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES (3-Key) Triple Data Encryption Algorithm (TDEA) Electronic Codebook (ECB), TDEA Cipher Block Chaining (CBC), TDEA Cipher Feedback (CFB)	168	FIPS 46-3 (cert #471)
	AES (128, 192, 256) ECB, CBC, and CFB128	128, 192, 256	FIPS-197 (cert #453)
Asymmetric encryption and decryption	RSA (up to 4096 bits)	1024, 1536, 2048, 3072, 4096	FIPS 186-2 for Sign/Verify (cert # 172)
	DSA ⁸	N/A	FIPS 186-2 (cert #183)
Message Digest	SHA ⁹ -1	N/A	FIPS 180-2 (cert #516)

⁸ DSA – Digital Signature Algorithm

⁹ SHA – Secure Hashing Algorithm

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
	SHA-256	N/A	FIPS 180-2 (cert #516)
	SHA-384	N/A	FIPS 180-2 (cert #516)
	SHA-512	N/A	FIPS 180-2 (cert #516)
	MD5 ¹⁰	N/A	RFC 1321
Message Authentication	HMAC ¹¹	256, 384, 512	FIPS-198 (cert #216)
Random Number Generation	ANSI ¹² X9.31 DRNG ¹³	N/A	X9.31 (cert #238)

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

¹⁰ MD – Message Digest

¹¹ HMAC – Hashed Message Authentication Code

¹² ANSI – American National Standards Institute

¹³ DRNG – Deterministic Random Number Generator

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*Web Access SFP*] on

[

Subjects: Users attempting to establish an interactive session with the TOE

Objects: User interface menu items, policies, Web Messenger inboxes, Web Messenger messages, user PKI¹⁴ keys, X.509 certificates, services, product features

Operations: All interactions between the subjects and objects identified above

].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*Web Access SFP*] to objects based on the following:

[

Subject attributes:

1. *User role*
2. *User ID*
3. *User's permissions*

and Object attributes:

1. *Permissions assigned to objects*
2. *Absence of permissions assigned to objects*

].

¹⁴ PKI – Public Key Infrastructure

FDP_ACF.1.2

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

[

1. If the subject is the Universal Server administrator, then access is granted.
2. If a subject requests access to an object which has no assigned permissions, then access is granted.
3. If a subject who is not a Universal Server administrator requests access to an object which has assigned permissions, the permissions of the subject are examined to determine if the subject has permission to access the object. If a match is found, access is granted.
4. If none of the above rules apply, access is denied.

].

FDP_ACF.1.3

The TSF shall explicitly allow access of subjects to objects based on **no additional rules** ~~the following additional rules: [assignment: rules, based on security attributes, that explicitly atisfies access of subjects to objects].~~

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on **no additional security attributes** ~~[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].~~

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

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [Email SFP] on

[

Subjects: External IT entities trying to send controlled email traffic through the TOE

Object: Controlled email traffic sent through the TOE to other subjects

Operations: Any operation the TOE can perform on controlled email traffic passing through the TOE

].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.**FDP_IFF.1.1**

The TSF shall enforce the [*Email SFP*] based on the following types of subject and information security attributes:

[

Subject attributes:

1. *Username*
2. *Display name*
3. *Status*
4. *Email address*
5. *PGP keys*
6. *Whole Disk Recovery Tokens*
7. *Date and time of last use*

Information attributes:

1. *Recipient address*
2. *Recipient domain*
3. *Recipient user group*
4. *Message is to mailing list*
5. *Recipient key mode*
6. *External user recipient delivery preference*
7. *Sender address*
8. *Sender domain*
9. *Sender user group*
10. *Sender key mode*
11. *Message header*
12. *Message subject*
13. *Message body*
14. *Message size*
15. *Encryption of any part or all of the message*
16. *Signing of any part of the message*

17. *Message attachment name*
 18. *Message attachment type*
 19. *Message is from mailing list*
 20. *Mailing list user count*
 21. *Application*
 22. *Service type*
 23. *Successful authentication of connected user*
 24. *Internet Protocol (IP) address of local connector*
 25. *Port of local connector*
-].

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: *[Evaluate the configured policy rules and allow controlled email traffic to flow if the result of the evaluation is “allow”, otherwise controlled email traffic flow is not permitted]*.

FDP_IFF.1.3

The TSF shall enforce **no additional information flow control SFP rules** the ~~[assignment: additional information flow control SFP rules]~~.

FDP_IFF.1.4

The TSF shall explicitly allow an information flow based on **no additional rules** the ~~following rules: [assignment: rules, based on security attributes, that explicitly satisfies information flows]~~.

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on **no additional rules** the ~~following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]~~.

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

6.2.4 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when *[at least one]* unsuccessful authentication attempt occurs related to *[administrator login]*.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met, surpassed], the TSF shall [generate an alert for all administrators the TOE is configured to notify, and report unsuccessful authentication attempts in the daily status email].

Dependencies: FIA_UAU.1 Timing of authentication

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

[

An administrator-defined quality metric of:

1. *One upper-case letter, one lower-case letter, one special character, and one number for user passphrases.*
2. *A minimum pre-defined strength metric of 25%, 50%, 65%, 75%, 80%, 85%, 90%, or 100% for PKI key passphrases.*

].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

The TSF shall allow [access to the Verified Directory interface] 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_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1

The TSF shall allow [*access to the Verified Directory interface*] 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

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to *[perform the actions listed under Permissions in Table 11 below]* the functions *[listed under Permissions in Table 11 below]* to *[the roles specified under Role in Table 11 below]*.

Table 11 – Management of Security Functions Behaviour

Role	Permissions
Read-Only Administrator	View all settings and logs
WDRT ¹⁵ -only Administrator	View all settings and logs, access and read Whole Disk Recovery Tokens
Service Control Only	View all settings and logs, start and stop software and hardware services but not configure them
Basic Administrator	View all settings and logs, control and configure services, access and read Whole Disk Recovery Tokens, configure system settings, install updates, restore backups, manage messaging policies, manage users and their public keys, and vet users
Full Administrator	View all settings and logs, control and configure services, access and read Whole Disk Recovery Tokens, configure system settings, install updates, restore backups, manage messaging policies, manage users and their public keys, vet users, configure clustering, export user private keys, and manage organization, trusted, ignition, and Additional Decryption Keys (ADKs)
SuperUser	View all settings and logs, control and configure services, access and read Whole Disk Recovery Tokens, configure system settings, install updates, restore backups, manage messaging policies, manage users and their public keys, vet users, configure clustering, export user private keys, and manage organization, trusted, ignition, and ADKs, access the PGP Universal Server via SSH, and create and manage other administrators

¹⁵ WDRT – Whole Disk Recovery Token

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

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*Web Access SFP and Email SFP*] to restrict the ability to [*manage*] the security attributes [*attributes relating to reporting, policies, users, mail, organization, services, and system*] to [*authorized administrators*].

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(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*Web Access SFP*] to restrict the ability to [*manage*] the security attributes [*allowed ciphers for PGP Keys*].

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.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [*all security attributes*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3(a) Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1(a)

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

FMT_MSA.3.2(a)

The TSF shall allow the [*authorized administrators*] 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(b) Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1(b)

The TSF shall enforce the [*Email SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b)

The TSF shall allow the [*authorized administrators*] 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_REV.1 Revocation

Hierarchical to: No other components.

FMT_REV.1.1

The TSF shall restrict the ability to revoke [*all security attributes*] associated with the [*users: associated public keys*] under the control of the TSF to [*authorized administrators*].

FMT_REV.1.2

The TSF shall enforce the rules [*Web Access SFP rules*].

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:

[

1. *Management of security functions behavior*
 2. *Management of security attributes*
-].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Read-Only Administrator, WDRT-only Administrator, Service Control Only, Basic Administrator, Full Administrator, SuperUser*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TOE Security Function

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

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*fifteen-minutes of inactivity*].

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL 2 conformant. Table 12 – Assurance Requirements summarizes the requirements.

Table 12 – Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM ¹⁶ system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.4 TOE Security Assurance Measures

EAL 2 was chosen to provide a basic level of independently assured security. This section of the Security Target maps the developer assurance requirements of the TOE for a CC EAL 2 level of assurance to the assurance measures used for the development and maintenance of the TOE by the developer. The following table provides a mapping of the appropriate documentation to the developer's TOE assurance requirements.

¹⁶ CM – Configuration Management

Table 13 – Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ALC_CMC.2	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Configuration Management
ALC_CMS.2	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Configuration Management
ALC_DEL.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Secure Delivery
ADV_ARC.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Development: Security Architecture, Functional Specification, and TOE Design
ADV_FSP.2	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Development: Security Architecture, Functional Specification, and TOE Design
ADV_TDS.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Development: Security Architecture, Functional Specification, and TOE Design
AGD_OPE.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 Administrator's Guide PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Guidance: Operational User Guidance Supplement
AGD_PRE.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 Administrator's Guide PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Guidance: Preparative Procedures Supplement
ATE_COV.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Functional Tests and Coverage

Assurance Component	Assurance Measure
ATE_FUN.1	PGP Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 – Functional Tests and Coverage

6.4.1 ALC_CMC.2: Use of a CM system, ALC_CMS.2: Parts of the TOE CM coverage

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at PGP. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.4.2 ALC_DEL.1: Delivery Procedures

The Delivery document provides a description of the secure delivery procedures implemented by PGP to protect against TOE modification during product delivery to the customer.

6.4.3 ADV_ARC.1: Security Architecture Description, ADV_FSP.2: Security-enforcing Functional Specification, ADV_TDS.1: Basic design

The PGP design documentation consists of several related design requirements that address the components of the TOE at different levels of abstraction. The following sections of the design document address the Development Assurance Requirements:

- The Security Architecture Description provides a description of the architecture-oriented features of domain separation, TSF self-protection, and non-bypassability of the security functionality.
- The Security-enforcing Functional Specification (FSP) provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose, method of use, parameters and parameter descriptions for each external TSF interface. In addition, the FSP describes all the direct error messages that may result from security enforcing effects. The FSP also provides a mapping from the FSP to the SFRs.
- The Basic Design provides a design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF for a relatively simple TOE. The basic design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and a mapping from the TSF interfaces of the FSP to the lowest level of decomposition available in the TOE design.

6.4.4 AGD_OPE.1: Operational User Guidance, AGD_PRE.1: Preparative Procedures

The Operational User Guidance provides information about the proper usage of the TOE in its evaluated configuration. This guidance is intended to be used by all types of users: end-users, persons responsible for maintaining and administering the TOE in a correct manner for maximum security, and by others (e.g., programmers) using the TOE's external interfaces. Operational User Guidance describes the security functionality provided by the TSF, provides instructions and guidelines (including warnings), helps users to understand the TSF, and includes the security-critical information, and the security-critical actions required, for its secure use.

The Preparative Procedures are used to ensure that the TOE has been received and installed in a secure manner as intended by the developer. The requirements for preparation call for a secure transition from the delivered TOE to its initial operational environment.

6.4.5 ATE_COV.1: Evidence of Coverage, ATE_FUN.1: Functional Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates that all TSFIs in the FSP have been tested.

Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

7.1 TOE Security Functions

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 14 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.3	Cryptographic Key Access
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(a)	Management of security attributes

TOE Security Function	SFR ID	Description
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3(a)	Static attribute initialization
	FMT_MSA.3(b)	Static attribute initialization
	FMT_REV.1	Revocation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination

7.1.1 Security Audit

The Universal Server Audit function generates audit records for all system events related to the following categories:

- Administration
- Backup
- Client
- Cluster
- Ignition Key
- Mail
- Postfix
- Update
- Verified Directory
- Web Messenger

These records are stored in the System Log. Event records can be sorted by the following information:

- Description of the event
- Date and time of the event

An authorized administrator can review the events stored in the System Log through the Administrative Interface.

An administrator can configure the TOE to send logs to a remote Syslog server for later analysis. Only logs from the administration, updates, clustering, backups, Web Messenger, Verified Directory, Postfix, mail, and some logs of generic services are sent to the remote Syslog server. Other logs can be exported manually to a text file. Logs that the TOE exports automatically are exported as they arrive in the System Log.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1

7.1.2 Cryptographic Support

The Cryptographic Support function provides encryption and decryption of emails transmitted through the TOE where:

- The TOE knows the recipient's private key (for decryption) or can find the recipient's public key (for encryption)
- Mail policy allows encryption or decryption operations to be performed on the message

The Cryptographic Support function provides digital signature and verification of emails transmitted through the TOE where:

- The TOE can find the sender's private key (for digital signing) or knows the sender's public key (for verification)
- Mail policy allows signing or verification operations to be performed on the message

Key generation is handled by a DRNG according to the X9.31 standard for generating cryptographic keys.

PGP keys have a preferred symmetric encryption algorithm associated with them. The preferred algorithm can be Triple-DES or AES. The symmetric algorithm uses its own randomly generated symmetric key to encrypt the PGP private key. Data encrypted "with" the PGP public key is actually encrypted using the symmetric algorithm and a randomly generated symmetric key. The symmetric key used to encrypt the data can only be decrypted with the private key of the recipient. The asymmetric algorithm used to encrypt the symmetric key is RSA as defined in FIPS 186-2 for Sign/Verify (cert # 172). The process of encrypting the symmetric key and sending the symmetric key (along with the encrypted data) to a recipient is known as key exchange. The TOE performs key exchange via email. All data (anything that is encrypted and not a symmetric key) is encrypted with the symmetric algorithm.

The Cryptographic Support function provides encryption and decryption of all data transmitted between the TOE and the management workstation. Management data is protected by the Secure Hypertext Transfer Protocol protocol. Usernames and passphrases are encrypted while being transmitted over the network.

The TOE can be configured to require an Ignition Key to boot. The Ignition Key is an ordinary PGP key pair Universal Server uses to protect itself on startup. When Universal Server is set to use a software Ignition Key, the administrator must enter the Ignition Secret passphrase (the passphrase used to encrypt the Ignition Key's private key) in order for the Universal Server to boot. If the Universal Server is set to use a hardware Ignition Key, then an administrator must connect an Athena ASEKey Universal Serial Bus (USB) token to the Universal Server hardware and enter the Ignition Secret passphrase for the Universal Server to boot. The USB token must hold a PGP key pair, placed there by PGP Desktop.

When the TOE backs up data, the backup file is protected during remote transfer by the Secure Copy protocol. Backups are encrypted with the administrator-configured preferred encryption algorithm, using a randomly-generated symmetric key that is encrypted with the Organization Key. The actual Organization Key pair is an ordinary PGP key pair that has been configured to be used as the Organization Key, and has no inherent special properties (the way the TOE uses the Organization Key makes the Organization Key unique). User and administrator usernames are stored in clear text, administrator passphrases are stored using a SHA-1 hash of the passphrase. Web Messenger passphrases are stored encrypted to the Ignition Secret (associated with the Ignition Key) using AES-256. If no Ignition Secret is defined on the server, Web Messenger user passphrases are stored as clear text.

The TOE uses X.509 certificates for various applications, including presenting authentication credentials to web clients of users connecting to the web interfaces, and signing X.509 certificates generated for users. X.509 is a cryptographic standard for PKI that specifies standard formats for public key certificates. For the Organization Certificate the TOE can use self-signed certificates or CA certificates.

Certificate Revocation Lists (CRLs) enable checking server and client certificates against lists provided and maintained by Cas that show certificates are no longer valid. The TOE administrator can import CRLs from trusted Cas and then use the CRLs to determine if the TOE's certificates are still valid.

The TOE's claimed cryptographic support is provided by a FIPS 140-2-validated cryptographic module in the TOE. The FIPS 140-2 certification for the TOE has been issued by the National Institute of Standards and Technology, certificate #1049.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.3, FCS_CKM.4, FCS_COP.1.

7.1.3 User Data Protection

The Universal Server allows authorized administrators to enforce a rigid policy for users and administrators accessing the TOE. SuperUser administrators can create administrative accounts for other administrators with one of six pre-defined privilege levels. During account creation, the SuperUser administrator sets the new administrator's default passphrase, account name, and email address. The SuperUser administrator can also flag whether or not the new administrator receives a daily status email. After the new administrator logs in, the new administrator can change his passphrase.

There is no way for an administrator to change his own role, or grant himself additional privileges. Privilege levels are pre-defined and only another SuperUser administrator can change them. SuperUser administrators cannot change their own permission level.

Using the Administrative Interface, administrators with appropriate permissions can craft policies to manage the email traffic. There are a large number of options available to manage email traffic, which provide enough flexibility to implement a wide variety of email policies. Policy rules can be chained together to enforce more complex rule sets on varying types of traffic. Email policies can also be crafted to discard email from certain sources or email with specified attachment file names and file types.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1.

7.1.4 Identification and Authentication

Universal Server users and administrators are identified by their usernames and authenticated via passphrases while connecting to the TOE through one of the web interfaces. Authentication is tied to the session, either the administrative session or the Web Messenger session.

The SuperUser administrator sets the default passphrase for each new administrator. Non-SuperUser administrators can change their own passphrases at any time (but they cannot change passphrases for other administrators). Administrators can set a user policy so that users creating accounts through the Web Messenger interface must use strong passphrases (containing at least one upper-case letter, one lower-case letter, one number, and one special character) and can enforce passphrase length from 0-99 characters. These passphrase settings can also apply to Web Messenger user passphrases.

Administrators or users can connect to three web interfaces. The Management Interface allows administrators to connect through a standard web browser to set up and configure the TOE. The Web Messenger Interface allows external users to connect and retrieve messages from the TOE in a protected environment when the TOE cannot send them encrypted to the external user. The Verified Directory Interface requires no authentication to access, however, if a user uploads or deletes a key from the Verified Directory service then a verification email is sent to that user before either of these operations is allowed to be performed.

If an administrator connected via the Management Interface or a user connected via the Web Messenger Interface is idle for a period exceeding fifteen minutes, the session is terminated. The user or administrator must login again before continuing to operate or configure the TOE.

If an administrator exceeds a pre-defined number of unsuccessful login attempts between 1 and 999, the TOE can be configured to generate an alert. The alert is displayed for all administrators configured to receive the alert message.

Email users are identified by their email addresses and authenticated via their associated key pairs. To associate a key pair with a user either an administrator must import that key pair into the TOE manually, or the TOE must generate the key pair for the user. The TOE can only access a user's private key if it is uploaded in SKM or SCKM. Keys uploaded in CKM or GKM do not provide a usable private key for Universal Server. Users may upload their public keys to the TOE through the Verified Directory service. If a user does not have a PKI key pair on the TOE, but the user uploads a public key, the TOE is able to authenticate the user's signature via the user's public key.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1.

7.1.5 Security Management

Universal Server is managed by administrators, who are assigned one of six roles. Each role grants a set of permissions to review and modify the configuration of the security attributes of the TOE. Administrator permissions are tied to the credentials used to authenticate an assigned role. All administrators are allowed to review such attributes as audit settings, network settings, and policies. Basic administrators and above can also modify the TOE configuration and define Email SFP Rules. Only the SuperUser role can create new administrators and modify settings of current administrators (except each administrator can change his own passphrase and email address). Only authorized administrators can manage the allowed ciphers for PGP keys.

During the initial setup of the TOE, a Setup Assistant guides the administrator through the initial configuration of the TOE, including creation of a SuperUser administrator account. Once the Setup Assistant finishes, the Setup Assistant role and function are no longer used. The Setup Console role allows for the specification of the IP address, subnet mask, server type (Primary, Secondary, keyserver, or restored), current date and time information, hostname, default gateway, Domain Name Service (DNS) servers, license information, default administrator account information, placement setup, mail server IP address, LDAP server IP address, ignition key setup, and Organization Key backup. Additional configurations must take place through the Administrative Interface.

The attributes integral to the Web Access SFP are restrictive by default. Only the default administrator account is configured for use after the initial setup. The default administrator account has SuperUser privileges and can configure accounts for other administrators after the initial setup.

The attributes integral to the Email SFP are permissive by default. After installation and until Learn Mode is deactivated, the Universal Server takes no action to encrypt outgoing email traffic.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.2, FMT_MSA.3(a), FMT_MSA.3(b), FMT_REV.1, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE provides reliable timestamp information for its own use. The TOE software retrieves the timestamp from the hardware clock, which is set during installation of the appliance. The order of the audit records can be determined by the value of the timestamps.

Administrators can set the time manually through the configuration settings. Administrators are assumed to be trusted and competent, and may change the system time whenever necessary.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.7 TOE Access

The TOE terminates an email user or administrative session after fifteen minutes or more of inactivity. Each time a login is completed, the inactivity-timeout value is updated. If the time since the last activity time exceeds fifteen minutes, the user or administrator is logged out.

TOE Security Functional Requirements Satisfied: FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1. There are no extended SFRs contained within this ST.

There are no protection profile claims for this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following tables provide detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 15 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication.	O.AUTHENTICATE counters this threat by ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
T.UNAUTH A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.LOG The TOE must record events of security relevance at the “not specified level” of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	O.LOG counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.

Threats	Objectives	Rationale
	<p>O.AUTHENTICATE</p> <p>The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication.</p>	<p>O.AUTHENTICATE counters this threat by ensuring that users are identified and authenticated prior to gaining access to TOE security data.</p>
<p>T.OPENRELAY</p> <p>An attacker who is not a TOE user may send multiple SMTP messages to the TOE, whose email addresses fall outside the set of addresses for which the TOE applies policies. The intent of this attack is to utilize the resources of the TOE to deliver bulk email on behalf of the originator.</p>	<p>O.MAILRVW</p> <p>The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.</p>	<p>O.MAILRVW counters this threat by ensuring that incoming emails are checked against a policy that determines the flow of email traffic.</p>
<p>T.AUDFUL</p> <p>An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.</p>	<p>OE.AUDIT_STORAGE</p> <p>The IT Environment will provide a means for secure storage of the TOE audit log files.</p>	<p>OE.AUDIT_STORAGE counters this threat by ensuring that the system log events are not modified or lost as a result of the actions of an attacker.</p>
<p>T.USRDATA</p> <p>An attacker who is not a TOE user could access individual email messages stored on the TOE, by viewing, sorting, or deleting the emails stored on the TOE.</p>	<p>O.AUTHENTICATE</p> <p>The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication.</p>	<p>O.AUTHENTICATE counters this threat by ensuring that external entities attempting to access data stored on the TOE be authenticated before that access is allowed.</p>
	<p>O.MESACC</p> <p>The TOE shall enforce an access control policy on TOE users who wish to access stored SMTP emails stored within the TOE.</p>	<p>O.MESACC counters this threat by ensuring that access to stored emails is controlled by an access control policy.</p>
<p>T.REMCONN</p> <p>An attacker who is not a TOE user may exploit network protocol(s) based vulnerabilities and compromise TOE services and data assets by establishing a remote connection to the TOE.</p>	<p>O.AUTHENTICATE</p> <p>The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication.</p>	<p>O.AUTHENTICATE counters this threat by ensuring that all TOE users must authenticate before being granted access to the TOE.</p>
	<p>O.ADMIN</p> <p>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.</p>	<p>O.ADMIN counters this threat by ensuring that only TOE users with appropriate privileges are allowed to access the management functions of the TOE.</p>

Threats	Objectives	Rationale
<p>T.NACCESS</p> <p>An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.</p>	<p>O.PKI_CRYPTO</p> <p>The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.</p>	<p>O.PKI_CRYPTO counters this threat by ensuring that traffic passing through the TOE is protected by a suite of PKI cryptographic functions ensuring the traffic's integrity and confidentiality.</p>
	<p>O.MAILRVW</p> <p>The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.</p>	<p>O.MAILRVW counters this threat by ensuring that email traffic passing through the TOE is passed through a set of policies dictating the level of protection needed for each message.</p>
<p>T.NMODIFY</p> <p>An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external entity.</p>	<p>O.PKI_CRYPTO</p> <p>The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.</p>	<p>O.PKI_CRYPTO counters this threat by ensuring that traffic passing through the TOE is protected by a suite of PKI cryptographic functions ensuring the traffic's integrity and confidentiality.</p>
	<p>O.MAILRVW</p> <p>The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.</p>	<p>O.MAILRVW counters this threat by ensuring that email traffic passing through the TOE is passed through a set of policies dictating the level of protection needed for each message.</p>
<p>T.NO_AUDIT</p> <p>A threat agent may perform security-relevant operations on the TOE without being held</p>	<p>O.TIMESTAMP</p> <p>The TOE must provide reliable timestamps for its own use.</p>	<p>O.TIMESTAMP counters this threat by ensuring that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.</p>

Threats	Objectives	Rationale
accountable for it.	O.LOG The TOE must record events of security relevance at the “not specified level” of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	O.LOG counters this threat by ensuring that an audit trail of management events on the TOE is generated.
	OE.AUDIT_STORAGE The IT Environment will provide a means for secure storage of the TOE audit log files.	OE.AUDIT_STORAGE counters this threat by ensuring that an audit trail of management events on the TOE is preserved and protected.
T.IA A threat agent may attempt to compromise the TOE by attempting actions that it is not authorized to perform on the TOE.	O.AUTHENTICATE The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication.	O.AUTHENTICATE counters this threat by ensuring that all administrators and email users authenticate before being allowed to access functionality on the TOE which requires authentication.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that any actions performed on the TOE are permitted only if requested by administrators with the appropriate privileges.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed and configured on the appropriate, dedicated hardware according to the appropriate installation guides.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely, including management of the audit trail.	OE.MANAGE upholds this assumption by ensuring that the TOE hardware and operating system support the TOE functions.

Assumptions	Objectives	Rationale
<p>A.MANAGE</p> <p>There are one or more competent administrators assigned to manage the TOE and the security of the information it contains.</p>	<p>OE.MANAGE</p> <p>Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely, including management of the audit trail.</p>	<p>OE.MANAGE upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.</p>
	<p>OE.AUDIT</p> <p>Authorized managers of the audit facilities must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.</p>	<p>OE.AUDIT upholds this assumption by ensuring that administrators assigned to manage the TOE will review the audit logs on a regular basis and take the appropriate actions when breaches of security are detected.</p>
	<p>OE.REVIEW</p> <p>The configuration of the TOE will be inspected on a regular basis to ensure that the configuration continues to meet the organization's security policies in the face of:</p> <ul style="list-style-type: none"> • Changes to the TOE configuration • Changes in the security objectives • Changes in the threats presented by the hostile network • Changes (additions and deletions) in the services available between the hostile network and the corporate network 	<p>OE.REVIEW upholds this assumption by ensuring that administrators assigned to manage the TOE will review the configuration on a regular basis to ensure that it accurately reflects the intended configuration.</p>
<p>A.NOEVIL</p> <p>The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.</p>	<p>OE.MANAGE</p> <p>Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely, including management of the audit trail.</p>	<p>OE.MANAGE upholds this assumption by ensuring that all users assigned to manage the TOE are non-hostile and follow all administrator guidance.</p>
<p>A.FIREWALL</p> <p>All ports needed for proper</p>	<p>OE.FIREWALL</p> <p>The Firewall must have all ports</p>	<p>OE.FIREWALL upholds the assumption by ensuring that all ports necessary for the operation of the</p>

Assumptions	Objectives	Rationale
operations of the TOE will be opened at the firewall.	needed for proper operations of the TOE opened.	TOE are opened.
A.DNS DNS information received by the TOE is reliable.	OE.TRUSTED_INFO Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.	OE.TRUSTED_INFO upholds this assumption by ensuring that DNS requests sent from the TOE cannot be disclosed or modified, and that DNS replies cannot be compromised.
A.DIRECT The TOE hardware is physically available to authorized administrators only.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT upholds this assumption by ensuring that the TOE environment provides protection from external interference or tampering.
	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	OE.PHYSICAL upholds this assumption by ensuring that the TOE environment provides suitable security precautions to make the TOE only available to authorized administrators.
A.SINGEN Email messages cannot pass between the internal and external networks without passing through the TOE.	OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN upholds this assumption by ensuring that the TOE environment directs emails through the TOE before allowing them to enter or leave the internal network.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to provide secure email proxy functions.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC upholds this assumption by ensuring that the TOE environment provides the TOE with the appropriate network configuration to perform secure email proxy functions.
A.PROTCT The TOE shall be protected from disruptions of TOE data and functions.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT upholds this assumption by ensuring that the TOE environment provides protection from external interference that may cause disruptions to TOE data and functions.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this Security Target.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this Security Target.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 – Objectives: Security Functional Requirements (SFRs) Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FAU_SAR.1	This requirement supports O.ADMIN by requiring the TOE to make the recorded audit records available for review.
	FIA_SOS.1	This requirement supports O.ADMIN by requiring the TOE to enforce a minimum strength for user passphrases.
	FIA_UID.1	This requirement supports O.ADMIN by ensuring the TOE users are identified before any other TSF-mediated actions that require authentication taken on the users' behalf are performed.
	FIA_UAU.1	This requirement supports O.ADMIN by ensuring that the TOE users are authenticated before any other TSF-mediated actions that require authentication taken on the users' behalf are performed.
	FMT_MOF.1	This requirement supports O.ADMIN by specifying which functions of the TOE can be managed, and defining who can manage those functions.
	FMT_MSA.1(a)	This requirement supports O.ADMIN by allowing all TOE administrators to manage the TOE security attributes.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.3(a)	This requirement supports O.ADMIN. The Web Access SFP is restrictive by default.
	FMT_REV.1	This requirement supports O.ADMIN by specifying how administrators may revoke email users' public keys.
	FMT_SMF.1	This requirement supports O.ADMIN by specifying that the TOE supports the management functions of the TOE.
	FMT_SMR.1	This requirement supports O.ADMIN by supporting six roles: Read-Only Administrator, WDRT-only Administrator, Service Control Only, Basic Administrator, Full Administrator, SuperUser
<p>O.AUTHENTICATE</p> <p>The TOE must require users to authenticate before gaining access to the TOE interfaces which require authentication.</p>	FIA_AFL.1	This requirement supports O.AUTHENTICATE by notifying administrators when a pre-configured number of failed login attempts is reached on an administrator account.
	FIA_UAU.1	This requirement supports O.AUTHENTICATE by requiring all TOE users to authenticate before any other TSF-mediated actions that require authentication taken on the users' behalf are performed.
	FIA_UID.1	This requirement supports O.AUTHENTICATE by ensuring the TOE users are identified before any other TSF-mediated actions that require authentication taken on the users' behalf are performed.
	FTA_SSL.3	This requirement supports O.AUTHENTICATE by ensuring TOE users are logged off after fifteen minutes of inactivity, ensuring that unauthenticated users do not gain access to the TOE through an unattended session.

Objective	Requirements Addressing the Objective	Rationale
<p>O.MAILRVW</p> <p>The TOE shall review all incoming and outgoing SMTP messages to determine that the defined policies are enforced and the appropriate actions are performed on every message.</p>	FDP_IFC.1	This requirement supports O.MAILRVW by including an administrator-configurable policy that enables the administrator to construct rules representing the site's information flow policy. The function then enforces those rules and takes the action specified.
	FDP_IFF.1	This requirement supports O.MAILRVW by supporting a wide range of attributes that can be used in the Email SFP to control the flow of email messages between the Internal and External Networks.
	FMT_MSA.1(a)	This requirement supports O.MAILRVW by allowing all TOE administrators to manage the TOE security attributes.
	FMT_MSA.3(a)	This requirement supports O.MAILRVW. The Web Access SFP is restrictive by default.
	FMT_MSA.3(b)	This requirement supports O.MAILRVW. The Email SFP is permissive by default.
<p>O.MESACC</p> <p>The TOE shall enforce an access control policy on TOE users who wish to access stored SMTP emails stored within the TOE.</p>	FDP_ACC.1	This requirement supports O.MESACC by including a configurable policy that enables administrators to construct rules that control the access of TOE users to the user interfaces that require authentication. The function then enforces those rules and takes the action specified.
	FDP_ACF.1	This requirement supports O.MESACC by supporting several attributes that can be used in the Web Access SFP to control access to the user interfaces.
	FMT_MSA.3(a)	This requirement supports O.MESACC. The Web Access SFP is restrictive by default.
<p>O.PKI_CRYPTO</p> <p>The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via</p>	FCS_CKM.1	This requirement supports O.PKI_CRYPTO by providing cryptographic key generation, which can be used to ensure cryptographic functionality on the TOE.

Objective	Requirements Addressing the Objective	Rationale
<p>encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.</p>	FCS_CKM.3	This requirement supports O.PKI_CRYPTO by providing a method to encrypt backup data from the TOE.
	FCS_CKM.4	This requirement supports O.PKI_CRYPTO by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorized person or IT entity.
	FCS_COP.1	This requirement supports O.PKI_CRYPTO by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing through or being stored on the TOE.
	FMT_MSA.1(b)	This requirement supports O.PKI_CRYPTO by ensuring that administrators can manage the secure values for security attributes.
	FMT_MSA.2	This requirement supports O.PKI_CRYPTO by ensuring that only secure values are accepted for security attributes.
	FMT_MSA.3(b)	This requirement supports O.PKI_CRYPTO. The Email SFP is permissive by default, but allows authorized administrators to set policies that allow the Email SFP to protect data transmitted by the TOE.
<p>O.TIMESTAMP</p> <p>The TOE must provide reliable timestamps for its own use.</p>	FPT_STM.1	This requirement supports O.TIMESTAMP by ensuring that the TOE provides a timestamp for the TOE's use.
<p>O.LOG</p> <p>The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.</p>	FAU_GEN.1	This requirement supports O.LOG by requiring the TOE to produce audit records for the system security events and for actions caused by enforcement of the Email SFP.
	FAU_SAR.1	This requirement supports O.LOG by requiring the TOE to make the recorded audit records available for review.

8.5.2 Security Assurance Requirements Rationale

EAL 2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL 2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 18 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 18 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
	FMT_MSA.2	✓	
FCS_CKM.3	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
	FMT_MSA.2	✓	
FCS_CKM.4	FCS_CKM.1	✓	
	FMT_MSA.2	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_MSA.2	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3(a)	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3(b)	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_SOS.1	No dependencies		
FIA_UAU.1	FIA_UID.1	✓	
FIA_UID.1	No dependencies		
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(b)	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.2	FDP_ACC.1	✓	
	FDP_IFC.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	
FMT_REV.1	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	No dependencies		
FTA_SSL.3	No dependencies		

9 Acronyms and Terminology

9.1 Acronyms

Table 19 – Acronyms

Acronym	Definition
ADK	Additional Decryption Key
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CFB	Cipher Feedback
CKM	Client Key Mode
CM	Configuration Management
CRL	Certificate Revocation List
DES	Digital Encryption Standard
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
FIPS	Federal Information Processing Standard
GB	Gigabyte
GKM	Guarded Key Mode
HMAC	Hashed Message Authentication Code
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SATA	Serial Advanced Technology Attachment
SCKM	Server-Client Key Mode

Acronym	Definition
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hashing Algorithm
SKM	Server Key Mode
SMSA	Self-Managing Security Architecture
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TDEA	Triple Data Encryption Algorithm
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
USB	Universal Serial Bus
WDRT	Whole Disk Recover Token

9.2 Terminology

Table 20 – Terminology

Term	Definition
Administrator	Any user who manages the TOE and its security configuration from within the internal network.
Email user	Any non-administrative user of the TOE.
External User	Any non-administrative user who uses the TOE from outside the Internal Network.
Internal User	Any non-administrative user who uses the TOE from inside the Internal Network.
User	Any administrative or non-administrative user of the TOE.