# Voltage SecureMail Suite 2.0
# EAL2
# Security Target

Release Date: May 4, 2007

Document ID: 05-797-R-0100

Version: 1.18

Prepared By: Ward Rosenberry
InfoGard Laboratories
641 Higuera Street, Second Floor
San Luis Obispo, CA 93401

Prepared For: Voltage Security
1070 Arastradero Road
Suite 100
Palo Alto, CA 94304

# Table of Contents

# List of Tables

# List of Figures

# 1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

## 1.1 Identification

TOE Identification: Voltage SecureMail Suite 2.0 in one of the following configurations:

TOE Configuration I

- Voltage SecurePolicy Suite version 2.0 on Windows 2003 Server with SP1
- Voltage SecureMail 2.0.5 for Outlook 2003 SP2 running on Windows 2000 with SP4 or Windows XP with SP2

TOE Configuration II

- Voltage SecurePolicy Suite version 2.0 on Windows 2003 Server with SP1
- Voltage SecureMail 2.0.5 for Outlook 2003 SP2 running on Windows 2000 with SP4 or Windows XP with SP2
- Voltage IBE Gateway Server version 2.0 on CentOS version 4.0

ST Identification: Voltage SecureMail Suite Version 2.0 EAL2 Security Target

ST Version: 1.18

ST Publish Date: May 4, 2007

ST Authors: Ward Rosenberry

PP Identification: N/A

## 1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.2[1] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.2 Part 3 conformant at EAL2.

The TOE is also compliant with all International interpretations with effective dates on or before September 22, 2005.

The TOE is compliant with selected NIAP Interpretations. The selected NIAP Interpretations are identified as they are applied to the security requirements in Section 5.

This TOE is not conformant to any Protection Profiles (PPs).

[1] Common Criteria (CC) for Information Technology Security Evaluation – January 2004, Version 2.2.

## 1.3 Overview

The Voltage SecureMail Suite 2.0 is a secure email system using identity-based encryption (IBE) that enables organizations to send secure, ad-hoc business communication such as financial statements, patient health information (PHI) or sensitive communication regarding intellectual property. The ability to conduct business electronically, while ensuring compliance with regulations such as GLBA (Gramm-Leach-Bliley Act) and HIPAA (Health Insurance Portability and Accountability Act) opens a number of business opportunities not possible before. For example, federal agencies may communicate securely via email with external entities such as contractors or suppliers without requiring pre-registration by external users.

## 1.4 Organization

| Section | Title | Description |
|---|---|---|
| 1 | Introduction | Provides an overview of the security target. |
| 2 | TOE Description | Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE. |
| 3 | TOE Security Environment | Contains the threats, assumptions and organizational security policies that affect the TOE. |
| 4 | Security Objectives | Contains the security objectives the TOE is attempting to meet. |
| 5 | IT Security Requirements | Contains the functional and assurance requirements for this TOE. |
| 6 | TOE Summary Specification | A description of the security functions and assurances that this TOE provides. |
| 7 | PP Claims | Protection Profile Conformance Claims |
| 8 | Rationale | Contains pointers to the rationales contained throughout the document. |

**Table 1: ST Organization and Description**

## 1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP Interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

**Assignment:** **indicated with bold text**

Selection: indicated with underlined text

***Refinement:*** ***additions indicated with bold text and italics***

~~***deletions indicated with strike-through bold text and italics***~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

Explicitly stated requirements claimed in this ST are denoted by the "_EXP" extension in the unique short name for the explicit security requirement.

## 1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

### 1.6.1 ST Specific Terminology

Identity-Based Encryption A public key system using an algorithm that can be used to turn a simple, well recognized identity such as an email address into a public/private key pair.

Voltage SecurePolicy Suite A subset of the Voltage SecureMail Suite that includes the Voltage Policy Server and Zero Download Messenger.

Policy Server A subset of the Voltage SecurePolicy Suite consisting of the Authentication Server, Server Management Console, Key Server, and Authentication Adapters. The Zero Download Messenger is not contained in the policy server. Note that this terminology refers to a collection of logical processes rather than a product.

Public Parameter Server A web server URL hosting the Voltage SecurePolicy Suite public parameters. This may be on the same system hosting the Voltage SecurePolicy Suite or a different system.

Voltage SecureMail Suite A complete TOE system consisting of the Voltage SecurePolicy Suite, the Voltage SecureMail plug-in, and (in TOE configuration II) the Voltage IBE Gateway Server.

Voltage SecureMail A client of the Voltage SecurePolicy Suite for handling user private keys that is implemented as a plug-in to Microsoft Outlook.

Voltage IBE Gateway Server A client of the Voltage SecurePolicy Suite within TOE configuration II that encrypts outgoing emails and decrypts incoming email messages on behalf of users. This component is also referred to as “the gateway” or the IBE gateway.

Zero Download Messenger A secure server (HTTPS) component of the Voltage SecurePolicy Suite that enables browser-based end users to read IBE-encrypted email messages without downloading and installing Voltage proprietary software.

### 1.6.2 Acronyms

| | |
|---|---|
| CC | Common Criteria |
| CLI | Command Line Interface |
| DMZ | Demilitarized Zone |
| FIPS | Federal Information Processing Specification |
| IBE | Identity-Based Encryption |
| PKI | Public Key Infrastructure |
| SFP | Security Functional Policy |
| SFR | Security Functional Requirement |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSC | TOE Scope of Control |
| TSF | TOE Security Function |
| TSFI | TOE Security Function Interface |
| TSP | TOE Security Policy |

# 2 TOE Description

## 2.1 Overview

The TOE is the Voltage SecureMail Suite version 2.0. The TOE is designed and manufactured by Voltage Security, Inc., 1070 Arastradero Road, Suite 100, Palo Alto, CA 94304, U.S.A., herein called Voltage.

The Voltage SecureMail Suite is a secure messaging TOE that provides end to end secure business communication (email) with application-level encryption. The Voltage SecureMail Suite leverages commonly existing email systems consisting of SMTP servers, Microsoft Outlook, and even browser-based email readers while avoiding the need for a supporting public key infrastructure (PKI) by using Identity Based Encryption (IBE). IBE, used with increasing frequency within government and business, uses well-known identities (in this case, globally unique email addresses) as public keys, eliminating the complexities of managing certificates, Certificate Revocation Lists (CRLs) and other costly infrastructure.

The IBE protocol is a public key system in which public parameters are published and available to all parties using IBE keys for purposes of identity-based encryption and decryption. Public key certificates are not needed to be maintained on each workstation as the identity of a key owner is the owner's globally unique email address. The public parameter is based on key material called a master secret that must be protected from discovery or modification. The system includes the mechanisms for protecting the master secret.

The system provides DSA keys for generation and verification of digital signatures applied to email messages for authentication purposes.

## 2.2 Architecture Description

The TOE (Configuration I) consists of a Voltage SecurePolicy Suite, and a Voltage SecureMail plug-in for Microsoft Outlook. TOE Configuration II adds an IBE Gateway Server.

The Voltage SecurePolicy Suite includes the Zero Download Messenger that may be used, if needed, by clients using only a web browser.

The Voltage Policy Server and the Voltage SecureMail plug-in for Microsoft Outlook email clients provide the minimum system configuration that provides the core functionality of the system, the ability to encrypt and decrypt email messages using IBE encryption and decryption. The Policy Server contains the following core functionality elements:

> An **Authentication Server** that ascertains the authentication status of users or administrators. The TOE does not contain its own system for authenticating users or system administrators but instead relies on external authentication methods such as Windows Domain Authentication, or local system credentials.

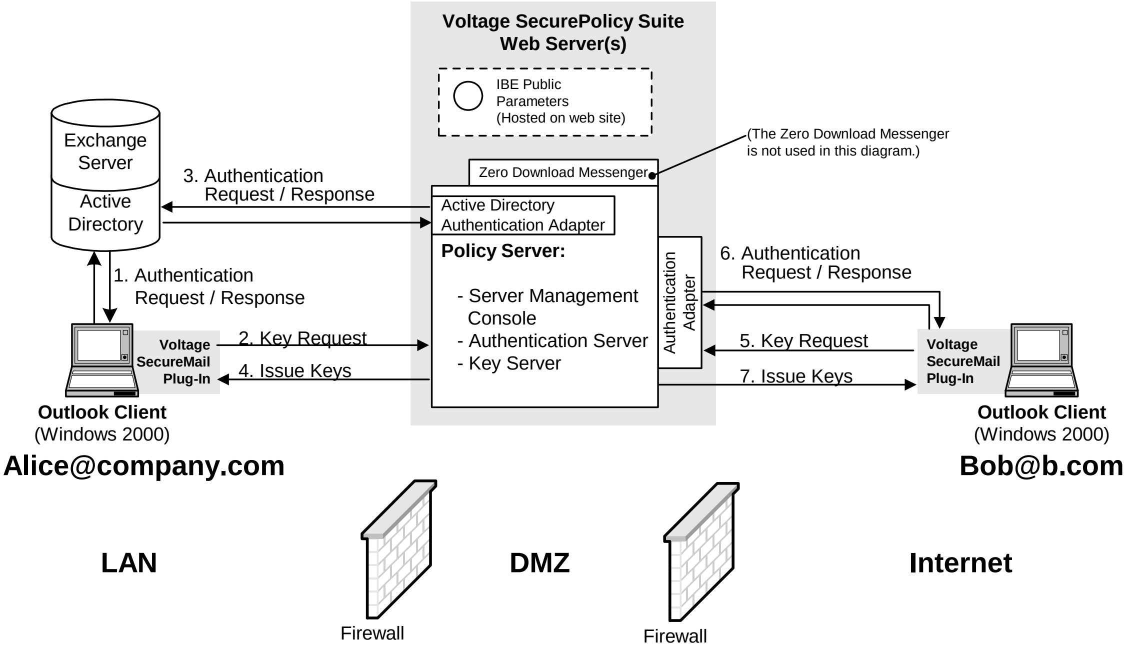
> A **Key Server** generates public/private key pairs using IBE (Identity-Based Encryption) cryptography. Public and private keys are generated on demand so there is no need for a private key server. Public keys may be stored within the system (in association with user names) for efficiency.
>
> A **Server Management Console** provides a GUI for administering the system. Administrators are authenticated if they are logged into the Windows Domain and they are included in a local administrative group (VoltageConfigAdmins or VoltageAuditAdmins) on the server.
>
> **Authentication Adapters** interface with enterprise authentication systems enabling the Policy Server to leverage enterprise authentication. The evaluated configuration uses the Microsoft Active Directory as the external authentication service provider.

The Voltage SecureMail plug-in for Microsoft Outlook integrates Voltage SecureMail Suite key management and usage capabilities with Microsoft Outlook Account Access functions, giving users the local abilities to encrypt and sign outgoing email messages, and to decrypt and verify signatures on incoming email messages.

The collection of Voltage SecurePolicy Suite and the Voltage SecureMail plug-in provides sufficient functionality to support end-to-end encryption between Microsoft Outlook clients as shown in Figure 1.

In the figure, the IBE public parameters are generated when the Voltage SecurePolicy Suite is first configured. These parameters are associated a particular server or *district* (a district is a particular server within a domain). All private keys generated by this key server are cryptographically related via the IBE public parameters such that signatures are unambiguously identified as coming from the district hosting the public parameters. Client systems use the IBE public parameters for signature validation purposes as well as the calculation of IBE public keys. The Voltage SecurePolicy Suite is installed in the DMZ (demilitarized zone), a sub-network between an internal trusted network and an external un-trusted public network. The Active Directory server provides Windows Domain Authentication credentials for users on the internal trusted network. Active Directory is part of the Microsoft Exchange server that provides email capabilities for the system.

## Figure 1 End-to-End Encryption and Decryption


Voltage SecurePolicy Suite Web Server(s)
IBE Public Parameters (Hosted on web site)
(The Zero Download Messenger is not used in this diagram.)
Zero Download Messenger
Exchange Server
Active Directory
3. Authentication Request / Response
Active Directory Authentication Adapter
Policy Server:
- Server Management Console
- Authentication Server
- Key Server
Authentication Adapter
6. Authentication Request / Response
1. Authentication Request / Response
2. Key Request
4. Issue Keys
5. Key Request
7. Issue Keys
Voltage SecureMail Plug-In
Voltage SecureMail Plug-In
Outlook Client (Windows 2000)
Outlook Client (Windows 2000)
Alice@company.com
Bob@b.com
LAN
DMZ
Internet
Firewall
Firewall

In this configuration that includes Microsoft Outlook clients provisioned with the Voltage SecureMail plug-in, Alice wants to send a message to Bob. When Alice clicks the Send Secure button on Outlook placed there by the SecureMail plug-in, several steps happen before the SecureMail plug-in encrypts the message using the IBE public parameters and Bob's email address (bob@b.com) as encryption input parameters.

1. When Alice logs on to her computer, her Windows session interacts with the Active directory to establish her domain credentials.
2. If Alice does not already have currently-valid IBE and DSA keys when she clicks the Send Secure button, the SecureMail plug-in sends an IBE key request and DSA certificate request over a Transport Layer Security (TLS v1) connection to the Voltage SecurePolicy Suite.
3. The Voltage SecurePolicy Suite authenticates Alice by checking her Windows domain credentials against the Active Directory service.
4. The key server generates the IBE private key and DSA public key certificate and returns these to her over the TLS connection.

   The SecureMail plug-in signs the message using Alice's DSA private key, encrypts the signed message using the public key for bob@b.com, and sends the encrypted and signed message to bob@b.com.
5. On receiving the encrypted and signed email, the SecureMail plug-in requests Bob's IBE private key and DSA keys from the key server (assuming he does not already have his keys). The request is passed using a TLS connection.
6. The Voltage SecurePolicy Suite authenticates Bob, using, in this case, the Question and Answer authentication adapter, which requires Bob to correctly

answer *m* of *n* questions. (Bob is in a domain that is outside the Active Directory domain so other authentication adapters (methods) must be used.)

7. The key server generates Bob's private IBE key and DSA certificate passing them to him over the TLS connection. Bob's SecureMail plug-in decrypts the message using Bob's private key as decryption input parameters.

   Bob's SecureMail plug-in verifies the digital signature on the signed payload using Alice's DSA certificate that was included in the secure message.

Additional TOE functionality is provided by the Zero Download Messenger. TOE Configuration II adds the Voltage IBE Gateway Server to TOE Configuration I.

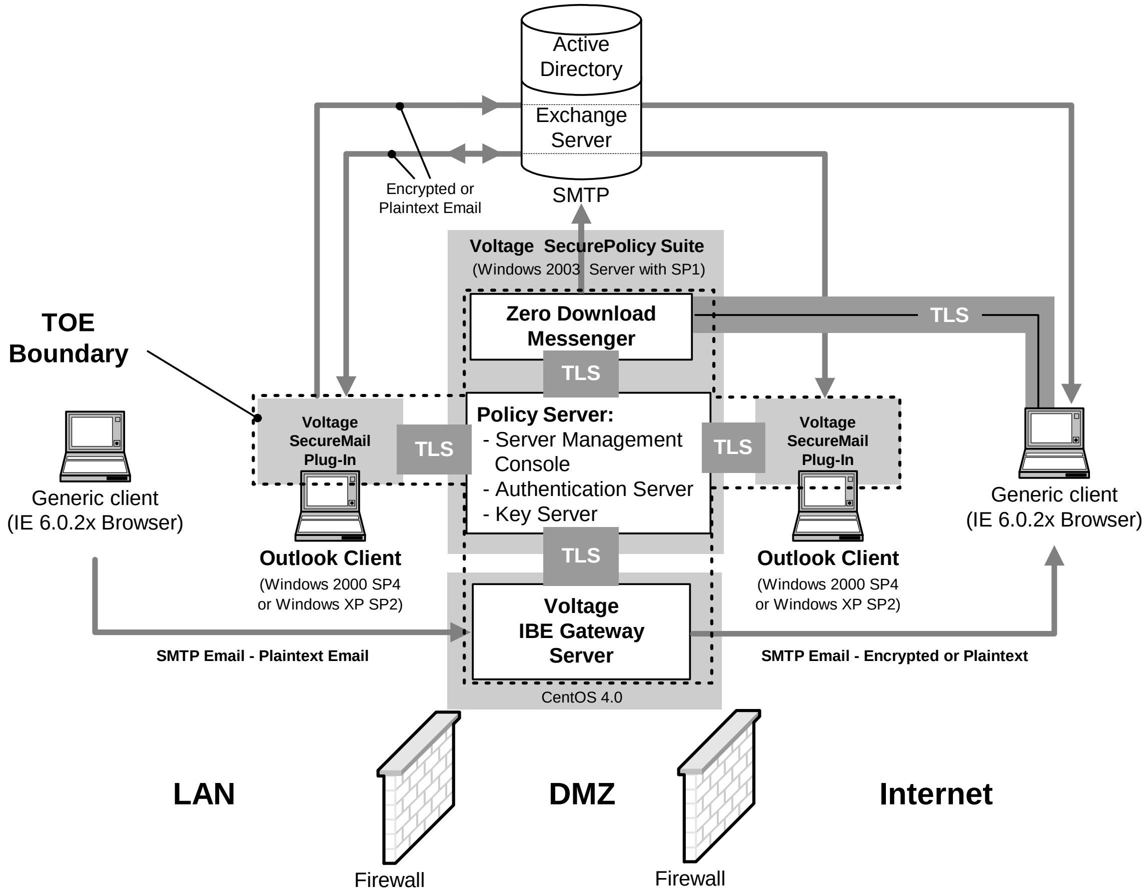
> The **Zero Download Messenger** (ZDM) relieves email clients from having to download any specialized client software onto their machine. All clients need is a browser (Internet Explorer version 6.x with 128-bit encryption enabled). When a client user receives an encrypted email, he or she clicks on an attachment that creates a TLS connection to the ZDM server. The ZDM server authenticates the client based on the policy defined in the Server Management Console. On success, the ZDM server requests the private key from the key server over a TLS connection established with the Key Server and uses the private key to decrypt Bob's email. ZDM offers the capability to reply or to save the decrypted message contents on the local machine. Note that no user data is ever saved on the ZDM. All email messages are saved in the client's mailbox where they remain the property of the recipient. In some configurations, as when all clients are provisioned with the SecureMail plug-in, the ZDM may be disabled.
>
> The **IBE Gateway** expands the Voltage SecureMail solution, letting organizations move decisions on whether to encrypt emails from users to the centralized server where enterprise policies can be enforced. The IBE Gateway is a rules-based encryption and decryption engine that enforces information flow policies, encrypting and decrypting email messages, based on sender and recipient identity, along with header and subject content.

## 2.3 Physical Boundaries

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the environment.

Figure 2 shows the full Voltage SecureMail Suite Configuration II that includes the Policy Server, Zero Download Messenger, Voltage SecureMail plug-in, and IBE Gateway Server.

**Figure 2 TOE Boundary**


Active Directory
Exchange Server
SMTP
Encrypted or Plaintext Email
Voltage SecurePolicy Suite
(Windows 2003 Server with SP1)
Zero Download Messenger
TLS
TLS
TOE Boundary
Voltage SecureMail Plug-In
TLS
Policy Server:
- Server Management Console
- Authentication Server
- Key Server
TLS
Voltage SecureMail Plug-In
Generic client
(IE 6.0.2x Browser)
Generic client
(IE 6.0.2x Browser)
TLS
Outlook Client
(Windows 2000 SP4 or Windows XP SP2)
Outlook Client
(Windows 2000 SP4 or Windows XP SP2)
Voltage IBE Gateway Server
SMTP Email - Plaintext Email
SMTP Email - Encrypted or Plaintext
CentOS 4.0
LAN
DMZ
Internet
Firewall
Firewall

The dashed line shows the TOE Boundary. Generic clients and browsers are in the environment, not in the TOE boundary. Similarly, Outlook Client system hardware and Outlook software reside in the environment while the SecureMail plug-in is inside the TOE boundary. The Active Directory is shown but not used in this example. See Figure 1 for a usage example. Not shown but implied in the figure is a web server component of the Voltage SecurePolicy Suite that supports HTTPS communications between the Voltage SecurePolicy Suite and distributed TOE subsystems and external TOE users.

TLS connections protect all sensitive data flows between distributed parts of the TOE.

### 2.3.1 Non-Bypassability of the TOE

TOE security functions cannot be bypassed as all interaction with the TOE security functions requires that user authentication be confirmed before the TOE allows access to security functions. Enforcement functions that confirm authentication status must succeed before TSF access is granted. Each TOE component (the Voltage SecurePolicy Suite, the Voltage SecureMail plug-in, and the IBE Gateway) includes a cryptographic module that is validated to FIPS 140-2 standards (see the FIPS module validation certificate 522). The cryptographic module includes a suite of FIPS self-tests including an integrity test that confirms the cryptographic module is not tampered or corrupted. The system gives an error and stops running if a tamper or corruption of this critical module is detected. The cryptographic module exists within each distributed TOE component. The Voltage SecureMail Suite is installed by an administrator with operating system access control permissions (within the environment) set to allow only authenticated administrators to add or remove the system or its components.

The TOE TSF maintains a separate domain for its execution to protect it from interference by outside (non-TSF) functions. The domain separation capability relies on process controls provided by the IT environment and by correct programming and use of pointers within the TOE components to ensure that user data and TSF data used for a TSF is correctly removed from memory before that TSF completes executing. This model prevents sensitive data from being inadvertently transmitted outside of the TOE. Finally, TOE distributed components employ TLS (transport layer security) to protect the integrity and confidentiality of data passing from one TOE component to another (even when components are on the same physical machine) or between a TOE component and a remote trusted IT product such as a web browser.

The TOE environment is further protected by adhering to the following checklists that are provided with the TOE installation guidance documentation.

1. In the evaluated configuration, Windows 2000 must be configured in accordanc with the following checklists:

   - DOT Windows 2000 Secure Baseline Configuration Standards
   - DISA Windows 2000 Security Checklist Version 4, Release 1.13
   - DISA Windows 2003/XP/2000 Addendum Version 5, Release 1

2. In the evaluated configuration, Windows Server 2003 must be configured in accordance with the following checklists:

   - DISA Windows Server 2003 Checklist Draft Version 4, Release 0.0
   - DISA Windows 2003/XP/2000 Addendum Version 5, Release 1

3. In the evaluated configuration, Windows XP must be configured in accordance with the following checklists:

   - Guide to Securing Microsoft Windows XP
   - DISA Windows XP Security Checklist Version 4, Release 1.13
   - DISA Windows 2003/XP/2000 Addendum Version 5, Release 1

### 2.3.2 Hardware Components

This table identifies required hardware components, all of which are in the environment and not part of the TOE.

| TOE or Environment | Component | Description |
|---|---|---|
| **For TOE Configuration I** | | |
| Environment | Server platform capable of running the Microsoft Windows 2003 Server operating system. | This is the server platform on which the Voltage SecurePolicy Suite executes. Minimally, this is a 2+ GHz server with at least 512 MB of RAM and 30 GB of free disk space, and Ethernet Network Interface Card (NIC). |
| Environment | PC or Workstation capable of running Windows 2000 SP4 or Windows XP SP2 and running Microsoft Outlook 2003. | This platform hosts the Voltage SecureMail plug-in for Microsoft Outlook. The hardware is a 75 MHz Intel Pentium processor, or above with at least 8 MB RAM, 2 MB disk space, a CD-ROM drive, and Ethernet Network Interface Card (NIC). |
| Environment | Any PC or Workstation capable of hosting Internet Explorer Version 6.x.x. | This platform hosts a web browser required for the use of ZDM. The hardware is a 75 MHz Intel Pentium processor, or above with at least 8 MB RAM, 2 MB disk space, a CD-ROM drive, and Ethernet Network Interface Card (NIC). |
| Environment | Server platform capable of running the Microsoft Windows 2003 Server operating system and the Microsoft Exchange Server 5.5. The Microsoft Exchange Server contains the Active Directory. | This is the server platform on which the Microsoft Exchange Server executes. Minimally, this is a 2+ GHz server with at least 512 MB of RAM and 30 GB of free disk space, and Ethernet Network Interface Card (NIC). |
| **For TOE Configuration II**<br>**Configuration II includes Configuration I and the following:** | | |

| | | |
|---|---|---|
| Environment | Server platform capable of running the CentOS 4.0, a Linux distribution derived from the Red Hat Linux 4 operating system. | This is the server platform on which the Voltage IBE Gateway executes. The hardware is 1.8 GHz Intel Pentium 4 processor, or above with 1 GB RAM − Recommended (512 MB RAM is the Minimum Requirement), 10 GB disk space, a CD-ROM drive and Ethernet Network Interface Card (NIC). |
| Environment | CD RW drive capable of writing a .iso image to a CD-ROM. | This is used to write the downloaded Voltage IBE Gateway and CentOS 4.0 image to a CD-ROM for the purpose of installing the image on the IBE Gateway server platform. |

**Table 2 Hardware Components**

### 2.3.3 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

| **TOE or Environment** | **Component** | **Description** |
|---|---|---|
| **For TOE Configuration I** | | |
| TOE | Voltage SecurePolicy Suite 2.0 | This component includes the Authentication Server, Server Management Console, Key Server, Authentication Adapter, and Zero Download Messenger. |
| Environment | Microsoft Windows 2003 Server with SP1 | This operating system underlies the Voltage SecurePolicy Suite. |
| Environment | MySQL Database Server 4.1.10a | This database software (provided with the TOE) holds TOE configuration data. |
| Environment | MySQL Connector 3.1.7 | This jar file (provided with the TOE) enables communication between the TOE and the database. |
| Environment | Java Runtime Environment (JRE) v1.4.2 | The JRE supports Java functions of the Voltage SecurePolicy Suite. |
| TOE | Voltage SecureMail 2.0.5 | This component manages encryption and decryption and signature generation and verification for end users. |
| Environment | Microsoft Outlook 2003 with SP2 | This component hosts Voltage SecureMail and enables users to access email messages. |
| Environment | Microsoft Windows 2000 with SP4 or Windows XP with SP2 | This operating system underlies the Microsoft Outlook Clients using the Voltage SecureMail plug-in. |

| | | |
|---|---|---|
| Environment | Microsoft Internet Explorer Version 6 or higher | This browser component is used on Microsoft Windows platforms to access the Zero Download Messenger component. |
| **For TOE Configuration II**<br>**Configuration II includes Configuration I and the following:** | | |
| TOE | Voltage IBE Gateway Server 2.0 | This component is a rules-based encryption and decryption appliance. |
| Environment | CentOS 4.0 − a Linux distribution derived from the Red Hat Linux 4 operating system | This operating system underlies the Voltage IBE Gateway. |

**Table 3 Software Components**

## 2.4 Logical Boundaries

This section contains the product features and denotes which are in the TOE. Examples are the following subsections.

### 2.4.1 Audit

The Voltage SecurePolicy Suite and the IBE Gateway have distinct auditing systems.

### *2.4.1.1 Voltage SecurePolicy Suite Audit*

The Voltage SecurePolicy Suite audit system records events from the Authentication Server, Server Management Console, Key Server, Identity Adapter, and Zero Download Messenger.

| | |
|---|---|
| **Audit Data Generation** | The TOE Voltage SecurePolicy Suite components generate audit records for the start-up and shut down of audit functions, administrator log in and log out, all decisions regarding key generation including key requests from the Zero Download Messenger and IBE Gateway, all security-relevant events and other non-security relevant events. |
| **User Identity Association** | Audit records include the identity of the user that caused the event. |
| **Audit Data Review** | The Voltage SecurePolicy Suite provides a graphical user interface to review audit records. Records may be searched using any of the following fields:<br>Time<br>Presumed subject identity or role<br>Event source<br>Log level (Error, Warning, Normal, Verbose, All) |

| | |
|---|---|
| | Session ID<br>Status |

#### *2.4.1.2 IBE Gateway Audit*

| | |
|---|---|
| **Audit data generation** | The TOE IBE Gateway components generate audit records for the start-up and shut down of audit functions, all decisions regarding encryption and decryption operations, all failed attempts to use a secret or private key, and all failed attempts to create a secure (TLS) connection. |
| **Audit data review** | The TOE IBE Gateway relies on operating system utilities grep and more to review audit messages. |

### 2.4.2 Communication

| | |
|---|---|
| **Selective proof of origin** | The TOE Voltage SecureMail plug-in for Microsoft Outlook provides digital signature generation and verification services. |

### 2.4.3 Cryptographic Support

| | |
|---|---|
| **Cryptographic key generation** | The TOE generates cryptographic keys in accordance with FIPS 140-2 standards. |
| **Cryptographic key destruction** | The TOE destroys cryptographic keys in accordance with FIPS 140-2 standards. |
| **Cryptographic operation** | The TOE performs cryptographic operations in accordance with FIPS and IEEE P1363.3 Standards. |

### 2.4.4 Identification and Authentication

| | |
|---|---|
| **User identification before any action** | The TOE and TOE environment ensures users are identified before allowing any user interactions with TOE security functions. |
| **User authentication before any action** | The TOE and TOE environment ensures users are authenticated before allowing any user interactions with TOE security functions |

### 2.4.5 Security Management

| | |
|---|---|
| **Management of security attributes** | The Voltage SecurePolicy Suite and the IBE Gateway administration interfaces enable authorized administrators to manage security attributes. |

| | |
|---|---|
| **Secure security attributes** | The TOE generates, uses, and destroys cryptographic keys in accordance with FIPS 140-2 standards to ensure they are secure security attributes. |
| **Specification of Management Functions** | The Voltage SecurePolicy Suite and the IBE Gateway administration interfaces enable authorized administrators to manage security functions. |
| **Security roles** | The Voltage SecurePolicy Suite maintains authorized configuration administrator and authorized audit administrator roles. The IBE Gateway supports a single administrator role. The Voltage SecureMail plug-in supports an implicit user role. |
| **Management of security attributes for the TOE environment** | The TOE environment provides management of security attributes. |
| **Management of TSF data** | The TOE Voltage SecurePolicy Suite and IBE Gateway limit the ability to manage TSF data to authorized administrators. |

### 2.4.6 Protection of the TSF

| | |
|---|---|
| **Reliable timestamps for TSF use** | The TOE environment provides reliable timestamps for use in auditing functions. |
| **Inter-TSF confidentiality during transmission** | The TOE uses TLS to provide confidentiality when communicating with remote IT products. |
| **Basic internal TSF data transfer protection** | The TOE uses TLS to provide confidentiality when communicating distributed parts of the TOE. |
| **Non-bypassability of the TSP** | The TOE and TOE environment contain features that prevent an attacker from bypassing the TSP. |
| **Domain Separation** | The TOE and TOE environment contain features that provide domain separation. |

## 2.5 Items Excluded from the TOE

The Voltage SecurePolicy Suite supports several identity adapters. The following are specifically excluded from the TOE:

- POP 3
- Remote Identity Adapter

The Voltage IBE Gateway has a decryption and re-encryption capability for the purposes of virus scanning or content scanning by an external application. This capability is specifically excluded from the TOE.

The Voltage Security Voltage SecureMail plug-in for Outlook includes a file wiping capability that is specifically excluded from the TOE.

# 3 TOE Security Environment

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the IT environment.

## 3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

### 3.1.1 Personnel Assumptions

A.ACCESS Only authorized IT administrators will have access to the servers on the TOE.

A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

A.USERDOCS TOE users will follow all guidance provided in the user documentation.

### 3.1.2 Physical Environment Assumptions

A.LOCATE The Voltage SecurePolicy Suite and IBE Gateway TOE components operate in a DMZ where they are subject to logical attack. The TOE is protected by a firewall with rules set to prevent unauthorized access to TOE resources.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.PHYSICAL It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

### 3.1.3 Operational Assumptions

A.AUDIT_BACKUP Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.

A.EXTSRVPROT The TOE interacts with external Microsoft Exchange and Active Directory servers. Secure TOE operation assumes IT administrators follow best practices to protect these external servers from attacks.

A.SECURE_COMMS It is assumed that the IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote operators.

## 3.2 Threats

The TOE or IT environment addresses the threats identified in this section. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.BYPASS An unauthorized person may attempt to bypass the security mechanisms of the IT environment so as to access and use security functions and/or non-security functions provided by the TOE.

T.USAGE The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

T.COMPROMISE An attacker may obtain or modify a private IBE or DSA key or secret AES or Triple-DES cryptographic key.

T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

T.SPOOF An unauthorized person may alter the sender address to send unauthorized data through the gateway.

T.MISUSE A TOE user may try to perform operations that are not permitted for that user. Such actions could cause the TOE to provide unintended assurances.

## 3.3 Organizational Security Policies

There are no organizational security policies for this TOE.

# 4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

## 4.1 Security Objectives for the TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.ACCESS The TOE will ensure that only those users with the correct authority are able to access a resource.

O.ACCOUN The TOE must provide user accountability for user data flows through the TOE, user acquisition of security attributes (private keys), and for authorized administrator use of security functions related to audit.

O.ALGS The TOE must implement cryptographic algorithms according to specified standards and, using cryptographic keys of a specified size, and perform cryptographic operations in accordance with specified algorithms.

O.AUDREC The TOE must provide a means to record a readable, searchable, and sortable audit trail of security related events, using accurate dates and times (drawn from the environment (see OE.TIME)).

O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

O.DESTROY The TOE must destroy secret and private keys according to FIPS 140-2 requirements.

O.IDENTITY The Voltage SecurePolicy Suite must be able to determine the identity of individual administrators and Zero Download Messenger users.

O.KEYGEN The TOE must generate cryptographic keys according to specified standards using FIPS 140-approved keys generation methods.

O.MANAGE The TOE will allow administrators to effectively manage the TOE, maintain it in a secure configuration, and allow management by authorized operators only.

O.MEDIAT The TOE mediates the application of TOE SFPs (security functional policies). These SFPs regulate Voltage SecureMail plug-in client acquisition and use of private keys to sign and decrypt email message objects. This objective requires the assurance that no residual information is transmitted.

O.PART_SEL_PRO The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces.

O.PROOF The TOE must allow Voltage SecureMail plug-in users to provide positive proof of having sent a message.

O.SECUREKEYS The TOE must provide a secure means to transfer secret and private keys between distributed parts of the TOE.

O.SECURE_COM The TOE must prevent user data from unauthorized disclosure while in transit between the TOE and remote trusted IT products or between distributed parts of the same TOE even when those parts are on the same platform.

## 4.2 Security Objectives for the Environment

The following IT security objectives for the environment are to be addressed by the IT environment by technical means.

OE.ACCOUN The IT environment must help provide user accountability for user data flows through the TOE and acquisition of security attributes (private keys).

OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

OE.DOMAIN_SEP The IT environment will provide an isolated domain for the execution of the TOE.

OE.GENPUR The Voltage IBE Gateway environment must provide general purpose utilities to enable selective viewing of audit records.

OE.I&A The environment will provide identification and authentication of individual TOE users.

OE.MANAGE The TOE environment provides administrative controls that enable an administrator to establish a secure execution environment for the TOE.

OE.MEDIAT The TOE environment mediates the application of the operating system access controls regulating acquisition and use of private keys.

OE.NO_BYPASS The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.

OE.TIME The TOE environment must provide accurate date and time information for use by TOE components.

The non-IT security objectives for the environment listed below are to be satisfied without imposing specific technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.

OE.PHYSEC Physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. TOE is physically secure.

## 4.3 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats, assumptions, and OSPs to the security objectives defined in this ST.

| | A.ACCESS | A.NO_EVIL | A.USERDOCS | A.LOCATE | A.PHYSICAL | A.LOWEXP | A.AUDIT_BACKUP | A.EXTSRVPROT | A.SECURE_COMMS | T.NOAUTH | T.BYPASS | T.USAGE | T.COMPROMISE | T.AUDACC | T.SPOOF | T.MISUSE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.GUIDAN | | | X | | | | X | | | | | X | | | | |
| O.ACCESS | | | | | | | | | | X | | | X | X | | |
| O.MANAGE | | | X | | | | X | | | | | X | | | | |
| O.AUDREC | | | | | | | | | | | | | | X | | |
| O.ACCOUN | | | | | | | | | | | | | | X | | |
| O.ALGS | | | | | | | | | | | | | X | | | |
| O.DESTROY | | | | | | | | | | | | | X | | | |

| | A.ACCESS | A.NO_EVIL | A.USERDOCS | A.LOCATE | A.PHYSICAL | A.LOWEXP | A.AUDIT_BACKUP | A.EXTSRVPROT | A.SECURE_COMMS | T.NOAUTH | T.BYPASS | T.USAGE | T.COMPROMISE | T.AUDACC | T.SPOOF | T.MISUSE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.IDENTITY | | | | | | | | | | | | | | X | | |
| O.KEYGEN | | | | | | | | | | | | | X | | | |
| O.SECUREKEYS | | | | | | | | | | | | | X | | | |
| O.SECURE_COM | | | | | | | | | X | | | | X | | | |
| O.MEDIAT | | | | | | | | | | | | | | | | X |
| O.PART_SEL_PRO | | | | | | | | | | X | | | | | | |
| O.PROOF | | | | | | | | | | | | | | | X | |
| OE.ACCOUN | | | | | | | | | | | | | | X | | |
| OE.GENPUR | | | X | | | | | | | | | | | X | | |
| OE.DOMAIN_SEP | | | | | | | | | | | X | | | | | |
| OE.I&A | | | | | | | | | | X | | | | X | | |
| OE.MANAGE | | | | | | | X | X | X | | | X | | | X | |
| OE.MEDIAT | | | | | | X | | | | X | | | | | | |
| OE.PHYSEC | X | | | X | X | X | | X | X | | | | | | | |
| OE.NOEVIL | | X | X | | | X | X | | X | | | | | | | |
| OE.ADMTRA | | X | X | | | | X | X | X | | | | | | | |
| OE.NO_BYPASS | | | | | | | | | | | X | | | | | |
| OE.TIME | | | | | | | | | | | | | | X | | |

**Table 4 – Threats & IT Security Objectives Mappings**

## 4.4 Rationale for Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.BYPASS

An unauthorized person may attempt to bypass the security of the IT environment to access and use security functions and/or non-security functions provided by the TOE.

OE.NO_BYPASS imposes barriers of sufficient robustness to prevent unauthorized access. OE.DOMAIN_SEP maintains a security domain within the IT environment for TOE execution that protects it from interference and tampering by untrusted subjects.

T.NOAUTH

An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

The objective O.ACCESS, directly counters this threat by ensuring that only those users with the correct authority are able to access a resource. Authentication adapters intercept all communications to the TOE and confirm authentication status before establishing a session. OE.MEDIAT helps counter the threat through application of the operating system access controls to regulate acquisition and use of private keys. OE.I&A helps counter the threat by authenticating individual TOE users.

The objective O.PART_SEL_PRO counters this threat by maintaining a domain for TSF execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces.

T.USAGE

The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

The objective O.GUIDAN counters this directly by providing complete and accurate instructions for installing the TOE in a secure manner. This is supported by O.MANAGE and OE.MANAGE that provides mechanisms for administrators to effectively manage the TOE and TOE environment, maintaining a secure configuration.

T.COMPROMISE

An attacker may obtain or modify a private IBE or DSA key or secret AES or Triple-DES cryptographic key.

O.ALGS counters this threat by implementing cryptographic algorithms according to specified standards and, using cryptographic keys of a specified size, and performing cryptographic operations in accordance with specified algorithms. O.KEYGEN ensures cryptographic keys used for cryptographic algorithms have adequate security to resist brute force attacks. O.SECUREKEYS helps counter the threat by providing a secure means (TLS) to transfer secret and private keys between distributed parts of the TOE. O.DESTROY helps counter the threat by using a FIPS approved method of zeroization to completely destroy cryptographic keys after use. O.ACCESS helps counter the threat by requiring authentication before allowing access to a private or secret cryptographic key. O.SECURE_COM helps counter the threat by protecting user data (including cryptographic keys) from disclosure during transit between the TOE and remote trusted IT products or between distributed parts of the same TOE even when those parts are on the same platform.

T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

O.AUDREC counters this threat by providing a means to record a readable audit trail of security related events, with accurate dates and times (taken from the environment (OE.TIME)), and a means to search and sort the audit trail based on relevant attributes. O.ACCESS helps counter the threat by ensuring that only legitimate users access TOE resources. O.ACCOUN helps counter the threat by ensuring accountability for all uses of TOE resources. O.IDENTITY helps counter the threat by ensuring the TOE can identify all Voltage SecurePolicy Suite administrators. OE.ACCOUN helps counter the threat by ensuring accountability for IBE Gateway uses of TOE resources. OE.GENPUR helps counters the threat by ensuring that tools are available to TOE administrators to read log files on the IBE Gateway. OE.I&A helps counter the threat by authenticating individual TOE users.

T.SPOOF An unauthorized person may alter the sender address to send unauthorized data through the gateway.

OE.MANAGE counters this threat by administrative controls that enable an administrator to establish a secure execution environment for the TOE. The administrative controls include the ability to configure the IBE Gateway to accept only outbound email messages from the Exchange (mail) server. The Gateway relies on the Exchange server to authenticate its users. O.PROOF partially counters this threat by allowing SecureMail plug-in users to provide positive proof of having sent a specific message.

T.MISUSE A TOE user may try to perform operations that are not permitted for that user. Such actions could cause the TOE to provide unintended assurances.

O.MEDIAT counters this threat by regulating the use of resources including private keys to encrypt and decrypt email message objects. Security functional policies provide the rules for resource usage to prevent their misuse.

## 4.5 Rationale for Organizational Policy Coverage

The TOE does not have any organizational security policies.

## 4.6 Rationale for Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

The non-IT security objectives for the environment not discussed below are, in part, a re-statement of the security assumptions. These security objectives are:

- OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.
- OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.
- OE.PHYSEC Physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. TOE is physically secure.

The justification for assumption coverage is as follows:

A.ACCESS Only authorized IT administrators will have access to the servers on the TOE. OE.PHYSEC satisfies this assumption.

A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance. OE.NOEVIL and OE.ADMTRA satisfy this assumption.

A.USERDOCS TOE users will follow all guidance provided in the user documentation. OE.NOEVIL, OE.ADMTRA, O.GUIDAN, and O.MANAGE satisfy this assumption. OE.GENPUR ensures administrators can read IBE Gateway log files as directed.

A.LOCATE Certain TOE components operate in a DMZ where they are subject to logical attack. The TOE is protected by a firewall The TOE is protected by a firewall with rules set to prevent unauthorized access to TOE resources. OE.PHYSEC satisfies this assumption.

A.PHYSICAL It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. OE.PHYSEC satisfies this assumption.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. OE.NOEVIL and OE.PHYSEC satisfy this assumption OE.PHYSEC and OE.MEDIAT establish barriers of sufficient robustness to prevent casual attacks.

A.AUDIT_BACKUP Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost. OE.NOEVIL, OE.ADMTRA, O.GUIDAN, O.MANAGE, and OE.MANAGE satisfy this assumption.

A.EXTSRVPROT The TOE interacts with external Microsoft Exchange and Active Directory servers. Secure TOE operation assumes IT administrators follow best practices to protect these external servers from attacks. OE.ADMTRA, OE.MANAGE, and OE.PHYSEC satisfy this assumption.

A.SECURE_COMMS It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote operators. OE.NOEVIL, OE.ADMTRA, O.SECURE_COM, OE.MANAGE, and OE.PHYSEC satisfy this assumption.

# 5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 - 5.3.1.

| **TOE Security Functional Requirements (from CC Part 2)** | |
|---|---|
| FCS_CKM.1a | Cryptographic key generation |
| FCS_CKM.1b | Cryptographic key generation |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1a | Cryptographic operations |
| FCS_COP.1b | Cryptographic operations |
| FCS_COP.1c | Cryptographic operations |
| FCS_COP.1d | Cryptographic operations |
| FCS_COP.1e | Cryptographic operations |
| FMT_MSA.2 | Secure security attributes |
| FPT_ITC.1 | Inter-TSF confidentiality during transmission |
| FPT_ITT.1 | Basic internal TSF data transfer protection |
| **Explicitly Stated TOE Security Functional Requirements** | |
| FAU_GEN_EXP.1a | Audit Data Generation for the Voltage SecurePolicy Suite |
| FAU_GEN_EXP.1b | Audit Data Generation for the IBE Gateway |
| FAU_GEN_EXP.2 | User Identity Association for the Voltage SecurePolicy Suite |
| FAU_SAR_EXP.1a | Audit Review for the Voltage SecurePolicy Suite |
| FAU_SAR_EXP.3 | Selectable Audit Review for the Voltage SecurePolicy Suite |
| FAU_SAR_EXP.1c | Audit Review for the IBE Gateway |
| FCO_NRO_EXP.1 | Selective proof of origin for the Voltage SecureMail plug-in |
| FCS_CKM_EXP.1a | Cryptographic key generation for the Policy Server-IBE keys |
| FCS_CKM_EXP.1b | Cryptographic key generation for the Policy Server-RSA keys |
| FCS_CKM_EXP.1c | Cryptographic key generation for the Policy Server-DSA keys |
| FCS_CKM_EXP.1d | Cryptographic key generation for the Voltage SecureMail plug-in Client |
| FCS_COP_EXP.1 | Cryptographic operations for the SecureMail Plug-In |
| FIA_UAU_EXP.2a | User authentication before any action for the Policy Server |
| FIA_UID_EXP.2a | User identification before any action for the Policy Server |
| FIA_UAU_EXP.2d | User authentication before any action for the IBE Gateway |
| FIA_UID_EXP.2d | User identification before any action for the IBE Gateway |
| FIA_UAU_EXP.2e | User authentication before any action for the Zero Download Messenger |
| FIA_UID_EXP.2e | User identification before any action for the Zero Download Messenger |
| FMT_MTD_EXP.1a | Management of TSF data for Certain TOE Components |
| FMT_MTD_EXP.1b | Management of TSF data for Certain TOE Components |
| FMT_SMR_EXP.1a | Security roles for Certain TOE Components |
| FMT_SMR_EXP.1b | Security roles for Certain TOE Components |
| FMT_SMR_EXP.1c | Security roles for Certain TOE Components |

| | |
|---|---|
| FPT_RVM_EXP.1a | Non-bypassability of the TSP when invoked by the OS |
| FPT_SEP_EXP.1a | Domain separation when invoked by the OS |
| **IT Environment Security Functional Requirements (from CC Part 2)** | |
| FDP_ACC.1 | Subset access control |
| FMT_MSA.1 | Management of security attributes |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security roles for the IT environment |
| FPT_STM.1 | Reliable time stamps for TSF use |
| **Explicitly Stated IT Environment Security Functional Requirements** | |
| FAU_SAR_EXP.1b | Audit Review by the IBE Gateway Environment |
| FIA_UAU_EXP.2b | User authentication before any action for the IBE Gateway environment |
| FIA_UAU_EXP.2c | User authentication before any action for the client environment |
| FIA_UID_EXP.2b | User identification before any action for the IBE Gateway environment |
| FIA_UID_EXP.2c | User identification before any action for the client environment |
| FPT_RVM_EXP.1b | OS Non-bypassability of the TSP |
| FPT_SEP_EXP.1b | OS TSF domain separation |

**Table 5 - Functional Requirements**

## 5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

### 5.1.1 Cryptographic Support (FCS)

#### *5.1.1.1 FCS_CKM.1 Cryptographic key generation*

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Advanced Encryption Standard (AES) symmetric keys** and specified cryptographic key sizes **128, 192, and 256-bits** that meet the following: **FIPS PUB 197.**

Dependencies:

FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_CKM.1.1b The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Triple Data Encryption Algorithm (Triple-DES) symmetric keys** and specified cryptographic key sizes **168 bits** that meets the following: **FIPS PUB 46-3**.

Dependencies:

FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

#### *5.1.1.2 FCS_CKM.4 Cryptographic key destruction*

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**.

Dependencies:

FCS_CKM.1 Cryptographic key generation

FMT_MSA.2 Secure security attributes

#### *5.1.1.3 FCS_COP.1 Cryptographic operation*

FCS_COP.1.1a The TSF shall perform **cryptographic key encryption and/or decryption** in accordance with a specified cryptographic algorithm **Identity Based Encryption (IBE) protocol** and cryptographic key sizes **1024 bits** that meet the following: **The draft IEEE P1363.3 on pairing-based cryptography**.

Dependencies:

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1b The TSF shall perform **data encryption and/or decryption** in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112 bits** that meet the following: **FIPS PUB 46-3**.

Dependencies:

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1c The TSF shall perform **data encryption and/or decryption** in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **128 bits** that meet the following: **FIPS PUB 197**.

Dependencies:

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1d The TSF shall perform **cryptographic key encryption and/or decryption,** in accordance with a specified cryptographic algorithm **RSA** and specified cryptographic key sizes **modulus 512 to 2048 bits** that meet the following: **PKCS#1 v1.5 and PKCS#1 v.1.5 with OAEP.**

Dependencies:

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1e The TSF shall perform **data hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **N/A** that meet the following: **FIPS 180-2 Secure Hash Standard (SHS)**.

Dependencies:

None

### 5.1.2 Security Management (FMT)

#### *5.1.2.1 FMT_MSA.2 Secure security attributes*

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

FDP_ACC.1 Subset access control

FMT_MSA.1 Management of security attributes

FMT_SMR_EXP.1 Security roles

### 5.1.3 Protection of the TSF (FPT)

#### *5.1.3.1 FPT_ITC.1 Inter-TSF confidentiality during transmission*

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies

#### *5.1.3.2 FPT_ITT.1 Basic internal TSF data transfer protection*

FPT_ITT.1.1 The TSF shall protect TSF data from **disclosure and modification** when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

## 5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

### 5.2.1 Security Audit (FAU)

#### *5.2.1.1 FAU_GEN_EXP.1a Audit Data Generation for the Voltage SecurePolicy Suite*

FAU_GEN_EXP.1.1a The TSF of the Voltage SecurePolicy Suite shall be able to generate an audit record of the following auditable events:

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

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

c) **All IBE key generation operations.**

FAU_GEN_EXP.1.2a The TSF of the Voltage SecurePolicy Suite shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, and **no other information**.

Dependencies:

FPT_STM.1 Reliable time stamps

### *5.2.1.2 FAU_GEN_EXP.1b Audit Data Generation for the IBE Gateway*

FAU_GEN_EXP.1.1b The TSF of the IBE Gateway shall be able to generate an audit record of the following auditable events:

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

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

c) **All usage of IBE keys for encryption and decryption purposes.**

FAU_GEN_EXP.1.2b The TSF of the IBE Gateway shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, and **no other information.**

Dependencies:

FPT_STM.1 Reliable time stamps

### *5.2.1.3 FAU_GEN_EXP.2 User Identity Association for the Voltage SecurePolicy Suite*

FAU_GEN_EXP.2.1 The TSF of the Voltage SecurePolicy Suite TOE component shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies:

FAU_GEN_EXP.1a Audit data generation

FIA_UID_EXP.2a Timing of identification

#### *5.2.1.4 FAU_SAR_EXP.1a Audit Review for the Voltage SecurePolicy Suite*

FAU_SAR_EXP.1.1a The TSF of the Voltage SecurePolicy Suite shall provide **authorized configuration administrators and authorized audit administrators** with the capability to read **all audit trail data** from the audit records.

FAU_SAR_EXP.1.2a The TSF of the Voltage SecurePolicy Suite shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies:
FAU_GEN_EXP.1a Audit data generation

#### *5.2.1.5 FAU_SAR_EXP.3 Selectable Audit Review for the Voltage SecurePolicy Suite*

FAU_SAR_EXP.3.1 The TSF of the Voltage SecurePolicy Suite shall provide the ability to perform searches of audit data based on:

**a) Time**

**b) Presumed subject identity or role**

**c) Event source**

**d) Log level (Error, Warning, Normal, Verbose, All)**

**e) Session ID**

**f) Status**

Dependencies:
FAU_SAR_EXP.1a Audit review

#### *5.2.1.6 FAU_SAR_EXP.1c Audit Review for the IBE Gateway*

FAU_SAR_EXP.1.1c The TSF of the IBE Gateway shall invoke services of the underlying host operating system to provide **authorized administrators** with the capability to read **all audit trail data** from the audit records.

FAU_SAR_EXP.1.2c The TSF of the IBE Gateway shall invoke services of the underlying host operating system to provide the audit records in a manner suitable for the user to interpret the information.

Dependencies:
FAU_GEN_EXP.1a Audit data generation

### 5.2.2 Communication (FCO)

#### *5.2.2.1 FCO_NRO_EXP.1 Selective proof of origin for the Voltage SecureMail plug-in*

FCO_NRO_EXP.1.1 The TSF of the Voltage SecureMail plug-in shall be able to generate evidence of origin for transmitted **email objects** at the request of the originator, and **no other parties**.

FCO_NRO_EXP.1.2 The TSF of the Voltage SecureMail plug-in shall be able to relate the **identity** of the originator of the information, and the **body of the message** of the information to which the evidence applies.

FCO_NRO_EXP.1.3 The TSF of the Voltage SecureMail plug-in shall provide a capability to verify the evidence of origin of information to the recipient, and no other parties upon receipt of the information.

Dependencies: FIA_UID_EXP.2c Timing of identification

## 5.2.3 Cryptographic Support (FCS)

### *5.2.3.1 FCS_CKM_EXP.1a Cryptographic key generation for the Policy Server – IBE Keys*

FCS_CKM_EXP.1.1a The TSF of the Policy Server shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Identity Based Encryption (IBE) asymmetric keys** and specified cryptographic key sizes **1024 bits** that meet the following: **Draft IEEE P1363.3 on pairing-based cryptography.**

Dependencies:

FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

### *5.2.3.2 FCS_CKM_EXP.1bCryptographic key generation for the Policy Server – RSA Keys*

FCS_CKM_EXP.1.1b The TSF of the Policy Server shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA asymmetric keys** and specified cryptographic key sizes **modulus 512 to 2048 bits** that meet the following: **FIPS 186-2 with Change Notice 1 dated October 5, 2001, Digital Signature Standard (DSS)**.

Dependencies:

FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

### *5.2.3.3 FCS_CKM_EXP.1c Cryptographic key generation for the Policy Server – DSA Keys*

FCS_CKM_EXP.1.1c The TSF of the Policy Server shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Digital Signature Algorithm (DSA) asymmetric keys** and specified cryptographic key sizes **modulus 1024 bits** that meet the following: **FIPS 186-2 with Change Notice 1 dated October 5, 2001, Digital Signature Standard (DSS)**.

Dependencies:

FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

#### *5.2.3.4 FCS_CKM_EXP.1d Cryptographic key generation for the Voltage SecureMail plug-in Client*

FCS_CKM_EXP.1.1d The TSF of the Voltage SecureMail plug-in client shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Digital Signature Algorithm (DSA) asymmetric keys** and specified cryptographic key sizes **modulus 1024 bits** that meet the following: **FIPS 186-2 with Change Notice 1 dated October 5, 2001, Digital Signature Standard (DSS)**.

Dependencies:

FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

#### *5.2.3.5 FCS_COP_EXP.1 Cryptographic operation for the SecureMail Plug-In*

FCS_COP_EXP.1.1 The TSF of the SecureMail plug-in shall perform **digital signature generation and/or verification** in accordance with a specified cryptographic algorithm **Digital Signature Algorithm (DSA)**, and cryptographic key sizes **modulus 1024-bits** that meet the following: **FIPS 186-2 with Change Notice 1 dated October 5, 2001, Digital Signature Standard (DSS)**.

Dependencies:

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

### 5.2.4 Identification and Authentication (FIA)

#### *5.2.4.1 FIA_UAU_EXP.2a User authentication before any action for the Policy Sever*

FIA_UAU_EXP.2.1a The TSF of the policy server shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:

FIA_UID_EXP.2a Timing of identification

#### *5.2.4.2 FIA_UID_EXP.2a User identification before any action for the Policy Sever*

FIA_UID_EXP.2.1a The TSF of the policy server shall require each user to identify itself before allowing any other TSF- mediated actions on behalf of that user.

Dependencies:

No dependencies

### *5.2.4.3 FIA_UAU_EXP.2d User authentication before any action for the IBE Gateway*

FIA_UAU_EXP.2.1d The TSF of the IBE Gateway when invoked by the underlying host environment shall require the administrative user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:

FIA_UID_EXP.2d Timing of identification

### *5.2.4.4 FIA_UID_EXP.2d User identification before any action for the IBE Gateway*

FIA_UID_EXP.2.1d The TSF of the IBE Gateway when invoked by the underlying host environment shall require the administrative user to identify itself before allowing any other TSF- mediated actions on behalf of that user.

Dependencies:

No dependencies

### *5.2.4.5 FIA_UAU_EXP.2e User authentication before any action for the Zero Download Messenger*

FIA_UAU_EXP.2.1e The TSF of the Zero Download Messenger shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:

FIA_UID_EXP.2e Timing of identification

### *5.2.4.6 FIA_UID_EXP.2e User identification before any action for the Zero Download Messenger*

FIA_UID_EXP.2.1e The TSF of the Zero Download Messenger shall require each user to identify itself before allowing any other TSF- mediated actions on behalf of that user.

Dependencies:

No dependencies

## 5.2.5 Security Management (FMT)

### *5.2.5.1 FMT_MTD_EXP.1 Management of TSF Data for Certain TOE Components*

FMT_MTD_EXP.1.1a The TSF of the Voltage SecurePolicy Suite shall restrict the ability to modify and **no other operations** the **TSF data listed in Table 4** to **authorized configuration administrator roles**.

| TSF Data | Description |
|---|---|
| Answers for the Q&A Adapter | Pairs of strings that correspond to the challenge presented to a user attempting to authenticate and the correct response. |
| key validity period | The time after which an IBE private key is valid. |
| Shared secret | A variable-length quantity whose length is configurable by the administrator. These values are shared between the policy server and the IBE Gateway and are passed as evidence of validity for interactions between the policy server and the gateway. |
| Cryptographic information | Generated by the administrator on initial configuration and when compromised. |
| Trusted districts | Names of email domains for which IBE public and private keys may be generated. Trusted districts limit the scope of users (email domains) that may access TOE security functions. |
| VSUser Exchange Directory Login Password | Administrator password needed to access the Exchange 5.5 directory server. The VSPS uses the password internally to access the Exchange Directory server. |
| ZDM Usernames and Passwords | Created by users during initial authentication to the Zero Download Messenger. |
| Public parameters | Public parameters that are needed for the operation of the IBE encryption. The server hosting them is verified by a TLS server certificate. |
| Client Policy | Information defining the operation of a Voltage IBE system. The server hosting them is verified by a TLS server certificate. |

**Table 6 - TSF Data for the Voltage SecurePolicy Suite**

Dependencies:

FMT_SMF.1 Specification of management functions

FMT_SMR_EXP.1a Security roles

FMT_MTD_EXP.1.1b The TSF ***of the IBE Gateway*** shall restrict the ability to modify and **no other operations** the **TSF data listed in Table 5** to **authorized administrator roles**.

| TSF Data | Description |
|---|---|
| Shared secret | A variable-length quantity whose length is configurable by the administrator. These values are shared between the policy server and the IBE Gateway and are passed as evidence of validity for interactions between the policy server and the gateway. |
| Security Functional Policy | Defines the rules by which the gateway decides to either encrypt or decrypt messages that it processes. |

**Table 7 - TSF Data for the Voltage IBE Gateway**

Dependencies:
FMT_SMF.1 Specification of management functions
FMT_SMR_EXP.1b Security roles

### *5.2.5.2 FMT_SMR_EXP.1 Security roles for Certain TOE Components*

FMT_SMR_EXP.1.1a The TSF of the Voltage SecurePolicy Suite shall maintain the roles **authorized configuration administrator, and authorized audit administrator,**.

FMT_SMR_EXP.1.2a The TSF of the Voltage SecurePolicy Suite shall be able to associate users with roles.

Dependencies: FIA_UID_EXP.2a User identification before any action

FMT_SMR_EXP.1.1b The TSF of the IBE Gateway shall maintain the role **authorized administrator**.

FMT_SMR_EXP.1.2b The TSF of the IBE Gateway shall be able to associate users with roles.

Dependencies: FIA_UID_EXP.2b User identification before any action

FMT_SMR_EXP.1.1c The TSF of the Voltage SecureMail plug-in shall maintain the role **authorized user**.

FMT_SMR_EXP.1.2c The TSF of the Voltage SecureMail plug-in shall be able to associate users with roles.

Dependencies: FIA_UID_EXP.2c User identification before any action

## 5.2.6 Protection of the TSF (FPT)

### *5.2.6.1 FPT_RVM_EXP.1a Non-bypassability of the TSP when invoked by the OS*

FPT_RVM_EXP.1.1a The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

#### *5.2.6.2 FPT_SEP_EXP.1a TSF domain separation when invoked by the OS*

FPT_SEP_EXP.1.1a The TSF, when invoked by the underlying host OS, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_EXP.1.2a The TSF, when invoked by the underlying host OS, shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

## 5.3 IT Environment Security Requirements

The SFRs defined in this section are based on similar requirements from Part 2 of the CC.

### 5.3.1 User Data Protection (FDP)

#### *5.3.1.1 FDP_ACC.1 Subset access control*

FDP_ACC.1.1 The ***IT environment*** shall enforce the **operating system access controls** on **all subjects (commands executing on behalf of users), objects (keys and data sent to the TOE or sent from the TOE for storage or use elsewhere), and operations (cryptographic operations performed by the TOE).**

Dependencies: No dependencies

### 5.3.2 Security Management (FMT)

#### *5.3.2.1 FMT_MSA.1 Management of security attributes*

FMT_MSA.1.1 The ***IT environment*** shall enforce the **group membership and file permissions** to restrict the ability to modify the security attributes **group membership and file permissions** to **authorized IT administrator roles**.

Dependencies: No dependencies

#### *5.3.2.2 FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1 The ***IT Environment*** shall be capable of performing the following security management functions: **management of group membership and file permissions**.

Dependencies: No dependencies

#### *5.3.2.3 FMT_SMR.1 Security roles for the IT environment*

FMT_SMR1.1 The ***IT Environment*** shall maintain the role **authorized IT administrator**.

FMT_SMR.1.2 The ***IT Environment*** shall be able to associate users with roles.

Dependencies: No dependencies

#### *5.3.2.4 FPT_STM.1 Reliable time stamps for TSF use*

FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time stamps for ***use by the TSF.***

Dependencies: No dependencies

## 5.4 Explicitly Stated IT Environment Security Functional Requirement

The SFRs on the IT environment defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

### 5.4.1 Security Audit (FAU)

#### *5.4.1.1 FAU_SAR_EXP.1b Audit Review by the IBE Gateway Environment*

FAU_SAR_EXP.1.1b The IBE Gateway environment shall provide authorized administrators with the capability to read all audit trail data from the audit records.

FAU_SAR_EXP.1.2b The IBE Gateway environment shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: No dependencies

### 5.4.2 Identification and Authentication (FIA)

#### *5.4.2.1 FIA_UAU_EXP.2b User authentication before any action for the IBE Gateway environment*

FIA_UAU_EXP.2.1b The IBE Gateway environment shall require each user to be successfully authenticated before allowing any TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

#### *5.4.2.2 FIA_UAU_EXP.2c User authentication before any action for the client environment*

FIA_UAU_EXP.2.1c The Voltage SecureMail plug-in client environment shall require each user to be successfully authenticated before allowing any TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

#### *5.4.2.3 FIA_UID_EXP.2b User identification before any action for the IBE Gateway environment*

FIA_UID_EXP.2.1b The IBE Gateway environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

#### *5.4.2.4 FIA_UID_EXP.2c User identification before any action for the client environment*

FIA_UID_EXP.2.1c The Voltage SecureMail plug-in client environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

### 5.4.3 Protection of the TSF (FPT)

#### *5.4.3.1 FPT_RVM_EXP.1b OS Non-bypassability of the TSP*

FPT_RVM_EXP.1.1b The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OS is allowed to proceed.

Dependencies: No dependencies

#### *5.4.3.2 FPT_SEP_EXP.1b OS TSF domain separation*

FPT_SEP_EXP.1.1b The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

FPT_SEP_EXP.1.2b The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

Dependencies: No dependencies

## 5.5 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users using the Zero Download Messenger and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria. The claimed minimum strength of function is SOF-basic. FIA_UAU_EXP.2e is the only non-cryptographic TOE security functional requirement that contains a permutational function.

## 5.6 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) as defined by the CC. The assurance components are summarized in the following table.

| Assurance Class | Assurance Components | |
|---|---|---|
| ACM: Configuration management | ACM_CAP.2 | Configuration items |
| ADO: Delivery and operation | ADO_DEL.1 | Delivery procedures |
| | ADO_IGS.1 | Installation, generation, and start-up procedures |
| ADV: Development | ADV_FSP.1 | Informal functional specification |
| | ADV_HLD.1 | Descriptive high-level design |
| | ADV_RCR.1 | Informal correspondence demonstration |
| AGD: Guidance documents | AGD_ADM.1 | Administrator guidance |
| | AGD_USR.1 | User guidance |
| ATE: Tests | ATE_COV.1 | Evidence of coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing - sample |
| AVA: Vulnerability assessment | AVA_SOF.1 | Strength of TOE security function evaluation |
| | AVA_VLA.1 | Developer vulnerability analysis |

**Table 8 - Assurance Requirements: EAL2**

### 5.6.1 ACM_CAP.2 Configuration items

*Developer action elements:*

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

*Content and presentation of evidence elements:*

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

*Evaluator action elements:*

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.2 ADO_DEL.1 Delivery procedures

*Developer action elements:*

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

*Content and presentation of evidence elements:*

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

*Evaluator action elements:*

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.3 ADO_IGS.1 Installation, generation, and start-up procedures

*Developer action elements:*

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

*Content and presentation of evidence elements:*

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

*Evaluator action elements:*

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

### 5.6.4 ADV_FSP.1 Informal functional specification

*Developer action elements:*

ADV_FSP.1.1D The developer shall provide a functional specification.

*Content and presentation of evidence elements:*

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

*Evaluator action elements:*

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

### 5.6.5 ADV_HLD.1 Descriptive high-level design

*Developer action elements:*

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

*Content and presentation of evidence elements:*

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

*Evaluator action elements:*

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 5.6.6 ADV_RCR.1 Informal correspondence demonstration

*Developer action elements:*

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

*Content and presentation of evidence elements:*

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

*Evaluator action elements:*

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.7 AGD_ADM.1 Administrator guidance

*Developer action elements:*

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

*Content and presentation of evidence elements:*

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

*Evaluator action elements:*

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.8 AGD_USR.1 User guidance

*Developer action elements:*

AGD_USR.1.1D The developer shall provide user guidance.

*Content and presentation of evidence elements:*

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

*Evaluator action elements:*

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.9 ATE_COV.1 Evidence of coverage

*Developer action elements:*

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

*Content and presentation of evidence elements:*

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

*Evaluator action elements:*

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.10 ATE_FUN.1 Functional testing

*Developer action elements:*

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

*Content and presentation of evidence elements:*

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

*Evaluator action elements:*

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.6.11 ATE_IND.2 Independent testing - sample

*Developer action elements:*

ATE_IND.2.1D The developer shall provide the TOE for testing.

*Content and presentation of evidence elements:*

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

*Evaluator action elements:*

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

### 5.6.12 AVA_SOF.1 Strength of TOE security function evaluation

*Developer action elements:*

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

*Content and presentation of evidence elements:*

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

*Evaluator action elements:*

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

### 5.6.13 AVA_VLA.1 Developer vulnerability analysis

*Developer action elements:*

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

*Content and presentation of evidence elements:*

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

*Evaluator action elements:*

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

## 5.7 Rationale for TOE Security Requirements

### 5.7.1 TOE Security Functional Requirements

| | O.ACCESS | O.ACCOUN | O.ALGS | O.AUDREC | O.DESTROY | O.GUIDAN | O.IDENTITY | O.KEYGEN | O.PART_SEL_PRO | O.PROOF | O.MANAGE | O.MEDIAT | O.SECUREKEYS | O.SECURE_COM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1a, b | | | | | | | | X | | | | | | |

| | O.ACCESS | O.ACCOUN | O.ALGS | O.AUDREC | O.DESTROY | O.GUIDAN | O.IDENTITY | O.KEYGEN | O.PART_SEL_PRO | O.PROOF | O.MANAGE | O.MEDIAT | O.SECUREKEYS | O.SECURE_COM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.4 | | | | | X | | | | | | | | | |
| FCS_COP.1a, b, c, d, e | | | X | | | | | | | | | | | |
| FMT_MSA.2 | | | X | | | | | | | | | | | |
| FPT_ITC.1 | | | | | | | | | | | | | X | X |
| FPT_ITT.1 | | | | | | | | | | | | | X | X |
| FAU_GEN_EXP.1a | | X | | X | | | | | | | | | | |
| FAU_GEN_EXP.1b | | | | X | | | | | | | | | | |
| FAU_GEN_EXP.2 | | | | | | | X | | | | | | | |
| FAU_SAR_EXP.1a | | | | X | | | | | | | | | | |
| FAU_SAR_EXP.1c | | | | X | | | | | | | | | | |
| FAU_SAR_EXP.3 | | | | X | | | | | | | | | | |
| FCO_NRO_EXP.1 | | | | | | | | | | X | | | | |
| FCS_CKM_EXP.1a, b | | | | | | | | X | | | | X | | |
| FCS_CKM_EXP.1c, d | | | | | | | | X | | | | | | |
| FCS_COP_EXP.1 | | | X | | | | | | | | | | | |
| FIA_UAU_EXP.2a | X | X | | | | | X | | | | | | | |
| FIA_UID_EXP.2a | X | X | | | | | X | | | | | | | |
| FIA_UAU_EXP.2d | X | X | | | | | | | | | | | | |
| FIA_UID_EXP.2d | X | X | | | | | | | | | | | | |
| FIA_UAU_EXP.2e | X | X | | | | | X | | | | | | | |
| FIA_UID_EXP.2e | X | X | | | | | X | | | | | | | |
| FMT_MTD_EXP.1a, b | X | | | | | X | | | | | X | | | |
| FMT_SMR_EXP.1a, b, c | | X | | | | | | | | | | | | |
| FPT_RVM_EXP.1a | | | | | | | | | X | | | | | |
| FPT_SEP_EXP.1a | | | | | | | | | X | | | | | |

**Table 9 – SFR and Security Objectives Mapping**

The following rationales ensure that SFRs trace back to objectives stated for the TOE. The rationales are organized by security objective.

O.ACCESS The TOE will ensure that only those users with the correct authority are able to access a resource.

The Policy Server interacts with the Active Directory to retrieve the user authentication data to determine user identity and authentication status [FIA_UAU_EXP.2a, FIA_UID_EXP.2a] before providing any services to the user, configuration administrator, or audit administrator including access to policy server TOE data [FMT_MTD_EXP.1a]. The IBE Gateway component requires the administrator to enter a username and password [FIA_UAU_EXP.2d, FIA_UID_EXP.2d] before providing any administrative services including access to IBE Gateway TOE data [FMT_MTD_EXP.1b]. The Zero Download Messenger requires the user to enter a username and password to identify and authenticate the user [FIA_UAU_EXP.2e, FIA_UID_EXP.2e] before providing any services to the user.

O.ACCOUN The TOE must provide user accountability for user data flows through the TOE, user acquisition of security attributes (private keys), and for authorized administrator use of security functions related to audit.

The audit records for the Voltage SecurePolicy Suite contain the identity of the user or administrator that caused the event [FAU_GEN_EXP.1a]. The Voltage TOE components (Voltage SecurePolicy Suite, Voltage SecureMail plug-in, and Voltage IBE Gateway) maintains roles [FMT_SMR_EXP.1a, FMT_SMR_EXP.1b, FMT_SMR_EXP.1c] and, in the case of the Voltage SecurePolicy Suite, associates human users with roles for the purpose of identifying users who cause audit events [FAU_GEN_EXP.1a]. The Policy Server confirms user and administrator identities before allowing any actions [FIA_UAU_EXP.2a, FIA_UID_EXP.2a]. The IBE Gateway associates the user identity with events caused by that user [FIA_UAU_EXP.2d, FIA_UID_EXP.2d]. The Zero Download Messenger associates the user identity with events caused by that user [FIA_UAU_EXP.2e, FIA_UID_EXP.2e].

O.ALGS The TOE must implement cryptographic algorithms following specified standards and, using cryptographic keys of a specified size, and perform cryptographic operations in accordance with specified algorithms.

The TOE uses standard (FIPS and IEEE P1363.3) cryptographic algorithms that can be confirmed they operate in the prescribed manner [FCS_COP.1a, b, c, d, e, and FCS_COP_EXP.1]. Following standards ensures that cryptographic algorithms provide adequate protection against disclosure of confidential information including cryptographic keys transferred via an encrypted channel [FMT_MSA.2].

O.AUDREC The TOE must provide a means to record a readable, searchable, and sortable audit trail of security related events.

The TOE generates audit records of security related events [FAU_GEN_EXP.1a, FAU_GEN_EXP.1b]. The audit records are readable so that the reader can interpret the information [FAU_SAR_EXP.1a]. The audit records are searchable, and sortable such that the reader may sort and search audit records based on event definitions and other audit-relevant information [FAU_SAR_EXP.3]. The audit records include timestamps drawn from the environment (see OE.TIME) that enable administrators to determine the chronological order of auditable events.

O.DESTROY The TOE destroys secret and private keys according to FIPS 140-2 requirements.

The TOE destroys cryptographic keys following standard practices (FIPS 140-2) to confirm they are completely removed from the system after use [FCS_CKM.4].

O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

The TOE includes guidance (documentation) that ensures the TOE is delivered, installed, administered, and operated in a manner that maintains security [FMT_MTD_EXP.1a, FMT_MTD_EXP.1b] . The TOE includes the required documentation [ADO_IGS, AGD_ADM, and AGD_USR].

O.IDENTITY The Voltage SecurePolicy Suite must be able to determine the identity of individual administrators and Zero Download Messenger users.

The TOE Voltage SecurePolicy Suite determines the identity of individual administrators and Zero Download Messenger users to correctly associate each auditable event with the identity of the administrator or user that caused the event [FAU_GEN_EXP.2]. The TOE requires each user to identify itself before allowing any TSF- mediated actions on behalf of that user [FIA_UAU_EXP.2a, FIA_UID_EXP.2a, FIA_UAU_EXP.2e, FIA_UID_EXP.2e].

O.KEYGEN The TOE must generate cryptographic keys according to specified standards using FIPS 140 approved or IEEE P1363.3 standard key generation methods.

The TOE generates cryptographic keys following the FIPS 140-2 or IEEE P1363.3 standard to ensure they possess the required properties [FCS_CKM.1a, b, FCS_CKM_EXP.1a, b, c, d]. Conformance to standards ensures that cryptographic keys are secure security attributes [FMT_MSA.2].

O.MANAGE The TOE will allow administrators to effectively manage the TOE, maintain it in a secure configuration, and allow management by authorized operators only.

The TOE restricts management of TSF data to authorized administrators [FMT_MTD_EXP.1a, FMT_MTD_EXP.1b]

O.MEDIAT The TOE mediates the application of TOE SFPs (security functional policies). These SFPs regulate Voltage SecureMail plug-in client acquisition and use of private keys to sign and decrypt email message objects. This objective requires the assurance that no residual information is transmitted.

The TOE enforces security functional policies for operations that generates or uses private IBE keys for use in decrypting email objects [FCS_CKM_EXP.1a] and that generates or uses private DSA keys for use in signing email objects [FCS_CKM_EXP.1b].

O.PART_SEL_PRO The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosures through its own interfaces.

The TOE provides a domain for its own execution that is free from external interference, tampering, or unauthorized disclosures [FPT_SEP_EXP.1a]. The TOE ensures TSF enforcement functions are invoked and succeed before each function may proceed [FPT_RVM_EXP.1a].

O.PROOF The TOE Voltage SecureMail plug-in allows its users to provide positive proof of having sent a message.

The TOE Voltage SecureMail plug-in component enables users to obtain and use a personal private DSA signing key to apply a digital signature to messages they send [FCO_NRO_EXP.1].

O.SECUREKEYS The TOE must provide a secure means to transfer secret and private keys between distributed parts of the TOE.

The TOE protects the privacy of cryptographic keys when they are transferred to remote trusted IT products [FPT_ITC.1]. The TOE protects the privacy of cryptographic keys when they are transferred to different parts of the TOE [FPT_ITT.1].

O.SECURE_COM The TOE must protect user data from unauthorized disclosure while in transit between the TOE and remote trusted IT products or between distributed parts of the same TOE even when those parts are on the same platform.

The TOE uses TLS sessions to protect user data from unauthorized disclosure while in transit between the TOE and remote trusted IT products [FPT_ITC.1] or while in transit between different parts of the TOE [FPT_ITT.1]. The TOE must provide a means to restrict management of TSF data to authorized administrators.

### 5.7.2 TOE Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

## 5.8 Rationale for IT Environment Security Requirements

| | OE.ACCOUN | OE.ADMTRA | OE.DOMAIN_SEP | OE.GENPUR | OE.I&A | OE.MANAGE | OE.MEDIAT | OE.NO_BYPASS | OE.TIME |
|---|---|---|---|---|---|---|---|---|---|
| FDP_ACC.1 | | | | | X | X | | | |
| FMT_MSA.1 | | | | | X | X | | | |
| FMT_SMF.1 | | | | | | X | X | | |
| FMT_SMR.1 | | | | | X | | X | | |
| FPT_RVM_EXP.1b | | | | | | | | X | |
| FPT_SEP_EXP.1b | | | X | | | | | | |
| FPT_STM.1 | | X | | | | X | | | X |
| FAU_SAR_EXP.1b | | | | X | | | | | |
| FIA_UAU_EXP.2b | | | | | | X | | | |
| FIA_UID_EXP.2b | | | | | | X | | | |
| FIA_UAU_EXP.2c | X | | | | | X | | | |
| FIA_UID_EXP.2c | X | | | | | X | | | |

**Table 10 – SFR and Security Objectives Mapping**

For the IT environment, the following rationales ensure that SFRs trace back to objectives stated for the environment. The rationales are organized by security objective.

OE.ACCOUN The TOE environment must help provide user accountability for user data flows through the TOE and acquisition of security attributes (private keys).

The TOE environment for the Voltage SecureMail plug-in Client provides identification and authentication of TOE users [FIA_UAU_EXP.2c, FIA_UID_EXP.2c]. Identity and authentication data is provided for use in auditable operations.

OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

Administrators recognize the security need to maintain accurate timestamps to enable accurate time information within audit records [FPT_STM.1].

OE.DOMAIN_SEP The IT environment will provide an isolated domain for the execution of the TOE.

The IT environment (the TOE underlying operating system) provides operator account facilities, access control mechanisms and correct use of memory management and pointers to provide an isolated domain for the execution of the TOE. [FPT_SEP_EXP.1b]

OE.NO_BYPASS The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.

The IT environment (the TOE underlying operating system) ensures that TOE operator authentication functions are invoked and succeed before each function within the TOE scope of control is allowed to proceed. [FPT_RVM_EXP.1b]

OE.I&A The environment will provide identification and authentication of all TOE users.

The Voltage SecureMail plug-in client environment provides identification of TOE users to control access to Voltage SecureMail plug-in functions [FDP_ACC.1]. The TOE environment on the Voltage SecurePolicy Suite host provides identification of TOE users to control access to Voltage SecurePolicy Suite user functions [FMT_MSA.1]. The TOE environment provides identification and authentication of IT administrators to regulate logical access to resources in the environment [FMT_SMR.1].

OE.MANAGE The TOE environment provides administrative controls that enable an administrator to establish a secure execution environment for the TOE.

The IT environment provides a robust access control mechanism (operating system access controls) [FDP_ACC.1]

The IT environment provides the utilities to manage security attributes (operating system access controls) [FMT_SMF.1].

The IT environment provides a robust login mechanism for user authentication [FIA_UAU_EXP.2b, FIA_UAU_EXP.2c].

The IT environment provides a robust login mechanism for user identification [FIA_UID_EXP.2b, FIA_UID_EXP.2c]

The IT environment provides administrative tools for managing permissions and group membership attributes [FMT_MSA.1].

The IT environment provides the utilities to set and provide accurate system time [FPT_STM.1].

OE.MEDIAT The TOE environment mediates the application of the operating system access controls regulating acquisition and use of private keys.

The TOE environment provides access control mechanisms consisting of file permissions [FMT_SMF.1], and access controls [FDP_ACC.1] to regulate access to the TOE resources.

OE.GENPUR The Voltage IBE Gateway environment must provide general purpose utilities to enable selective viewing of audit records.

The IT environment on the system hosting the IBE Gateway provides the general purpose utilities **more**, **grep**, **vi, and emacs** for use in viewing audit logs [FDP_SAR_EXP.1b].

OE.TIME The TOE environment must provide accurate date and time information for use by TOE components.

The IT environment provides accurate date and time information to be used by the auditing system [FPT_STM.1].

## 5.9 Rationale for Explicitly Stated Security Requirements

Table 11 presents the rationale for the inclusion of the explicit requirements found in this Security Target. The explicit security functional requirements stated for the TOE and the TOE environment do not bring any additional assurance measures into the evaluation.

| Explicit Requirement | Identifier | Rationale |
|---|---|---|

| Explicit Requirement | Identifier | Rationale |
|---|---|---|
| FAU_GEN_EXP.1a<br>FAU_GEN_EXP.1b | Distinct audit record contents | These explicit SFRs are needed to specify functionality that pertains to individual TOE components and not the TOE as a whole. |
| FAU_GEN_EXP.2 | Limited User Identity | This explicit SFR is needed to specify functionality that pertains to an individual TOE component and not the TOE as a whole |
| FAU_SAR_EXP.1a<br>FAU_SAR_EXP.1b<br>FAU_SAR_EXP.1c | Limited audit review capabilities | These explicit SFRs are needed to specify authentication functionality that pertains to TOE components or the TOE environment (FAU_SAR_EXP.1b) and not the TOE as a whole. |
| FAU_SAR_EXP.3 | Limited selectable audit review capabilities | This explicit SFR is needed to specify functionality that pertains to an individual TOE component and not the TOE as a whole. |
| FCO_NRO_EXP.1 | Limited non-repudiation of origin. | This explicit SFR is needed to specify functionality that pertains to an individual TOE component and not the TOE as a whole. |
| FCS_CKM_EXP.1a<br>FCS_CKM_EXP.1b<br>FCS_CKM_EXP.1c<br>FCS_CKM_EXP.1d | Limited cryptographic key generation | These explicit SFRs are needed to specify functionality that pertains to TOE components and not the TOE as a whole. |
| FCS_COP_EXP.1 | Limited use of a cryptographic operation | This explicit SFR is needed to specify functionality that pertains to an individual TOE component and not the TOE as a whole. |
| FIA_UAU_EXP.2a<br>FIA_UAU_EXP.2b<br>FIA_UAU_EXP.2c<br>FIA_UAU_EXP.2d<br>FIA_UAU_EXP.2e | Limited user authentication | These explicit SFRs are needed to specify authentication functionality that pertains to TOE components or the TOE environment (FIA_UAU_EXP.2b and FIA_UAU_EXP.2c) and not the TOE as a whole. |
| FIA_UID_EXP.2a<br>FIA_UID_EXP.2b<br>FIA_UID_EXP.2c<br>FIA_UID_EXP.2d<br>FIA_UID_EXP.2e | Limited user identification | These explicit SFRs are needed to specify identification functionality that pertains to individual TOE components or the TOE environment (FIA_UID_EXP.2b, and FIA_UID_EXP.2c) and not the TOE as a whole. |
| FMT_MTD_EXP.1a<br>FMT_MTD_EXP.1b | Limited management of TSF data | These explicit SFRs are needed to specify functionality that pertains to individual TOE components and not the TOE as a whole. |

| Explicit Requirement | Identifier | Rationale |
|---|---|---|
| FMT_SMR_EXP.1a<br>FMT_SMR_EXP.1b<br>FMT_SMR_EXP.1c | Limited provision of roles | These explicit SFRs are needed to specify functionality that pertains to individual TOE components and not the TOE as a whole. |
| FPT_RVM_EXP.1a<br>FPT_RVM_EXP.1b | Non-bypassability of the TOE and the TOE environment. | These explicit SFRs are needed to specify non-bypassability of the TOE and the TOE environment. |
| FPT_SEP_EXP.1a<br>FPT_SEP_EXP.1b | Domain separation provided by the TOE and the TOE environment. | These explicit SFRs are needed to specify domain separation that is provided by the TOE and the TOE environment. |

**Table 11 – Explicitly Stated SFR Rationale**

## 5.10 Rationale for IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

| Functional Component | Dependency | Included |
|---|---|---|
| FAU_GEN_EXP.1a | FTP_STM.1 | YES |
| FAU_GEN_EXP.1b | FTP_STM.1 | YES |
| FAU_GEN_EXP.2 | FAU_GEN_EXP.1a<br>FIA_UID_EXP.2a | YES<br>YES |
| FAU_SAR_EXP.1a | FAU_GEN_EXP.1a | YES |
| FAU_SAR_EXP.1b | FAU_GEN_EXP.1b | YES |
| FAU_SAR_EXP.3 | FAU_SAR_EXP.1a | YES |
| FAU_SAR_EXP.1c | FAU_GEN_EXP.1b | YES |
| FCO_NRO_EXP.1 | FIA_UID_EXP.2c | YES |
| FCS_CKM.1a | FCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES<br>YES<br>YES |
| FCS_CKM.1b | FCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES<br>YES<br>YES |
| FCS_CKM.4 | FCS_CKM.1<br>FMT_MSA.2 | YES<br>YES |
| FCS_CKM_EXP.1a | FCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES<br>YES<br>YES |
| FCS_CKM_EXP.1b | FCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES<br>YES<br>YES |

| **Functional Component** | **Dependency** | **Included** |
|---|---|---|
| FCS_CKM_EXP.1c | FCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES<br>YES<br>YES |
| FCS_CKM_EXP.1d | FCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES<br>YES<br>YES |
| FCS_COP.1.1a | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES (all iterations)<br>YES<br>YES |
| FCS_COP.1.1a | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES (all iterations)<br>YES<br>YES |
| FCS_COP.1.1b | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES (all iterations)<br>YES<br>YES |
| FCS_COP.1.1c | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES (all iterations)<br>YES<br>YES |
| FCS_COP.1.1d | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES (all iterations)<br>YES<br>YES |
| FCS_COP.1.1e | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | No<br>The only cryptographic function included in this iteration is a message digest which does not use keys. So these dependencies do not apply since they provide for key management, which is not required to provide message digest verification. |
| FCS_COP_EXP.1 | FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | YES (all iterations)<br>YES<br>YES |
| FDP_ACC.1 | FDP_ACF.1 | No.<br>As FDP_ACC.1 is an SFR in the environment, its dependencies are outside the scope of the TOE. |
| FIA_UAU_EXP.2a | FIA_UID_EXP.2a | YES |
| FIA_UAU_EXP.2b | FIA_UID_EXP.2b | YES |
| FIA_UAU_EXP.2c | FIA_UID_EXP.2c | YES |
| FIA_UAU_EXP.2d | FIA_UID_EXP.2d | YES |
| FIA_UAU_EXP.2e | FIA_UID_EXP.2e | YES |
| FIA_UID EXP.2a | None | N/A |
| FIA_UID EXP.2b | None | N/A |
| FIA_UID EXP.2c | None | N/A |
| FIA_UID EXP.2d | None | N/A |
| FIA_UID EXP.2e | None | N/A |

| Functional Component | Dependency | Included |
|---|---|---|
| FMT_MTD_EXP.1a | FMT_SMF.1<br>FMT_SMR_EXP.1a | YES<br>YES |
| FMT_MTD_EXP.1b | FMT_SMF.1<br>FMT_SMR_EXP.1b | YES<br>YES |
| FMT_MSA.1 | FDP_ACC.1<br>FMT_SMF.1<br>FMT_SMR.1 | NO<br>As FMT_MSA.1 is an SFR in the environment, its dependencies are outside the scope of the TOE. |
| FMT_MSA.2 | ADV_SPM.1<br>FDP_ACC.1<br>FMT_MSA.1<br>FMT_SMR.1 | N/A [1]<br>YES<br>YES<br>YES |
| FMT_SMF.1 | None | N/A |
| FMT_SMR.1 | None | N/A |
| FMT_SMR_EXP.1a | FIA_UID_EXP.1a | Substituted FIA_UID_EXP.2a |
| FMT_SMR_EXP.1b | FIA_UID_EXP.1b | Substituted FIA_UID_EXP.2b |
| FMT_SMR_EXP.1c | FIA_UID_EXP.1c | Substituted FIA_UID_EXP.2c |
| FPT_ITC.1 | None | N/A |
| FPT_ITT.1 | None | N/A |
| FPT_RVM_EXP.1a | None | N/A |
| FPT_RVM_EXP.1b | None | N/A |
| FPT_SEP_EXP.1a | None | N/A |
| FPT_SEP_EXP.1b | None | N/A |
| FPT_STM.1 | None | N/A |

**Table 12 – SFR Dependencies**

[1] ADV_SPM.1 is not necessary for this Security Target as the evaluation has shown the TOE maintains cryptographic keys in a secure state without requiring additional proof of ADV_SPM.1.

## 5.11 Rationale for Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Table 12 – SFR Dependencies
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.7.1
- including the SFRs for the environment FPT_SEP.1 and FPT_RVM.1 to protect the TSF

- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely

## 5.12 Rationale for Strength of Function Claim

The threats identified for this TOE assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation. Consequently, the strength of function level is SOF-basic. The TOE contains a non-cryptographic, probabilistic mechanism and AVA_SOF.1 is provided to satisfy this claim.

# 6 TOE Summary Specification

This section describes the TOE security functions and the security assurance measures.

## 6.1 TOE Security Functions

### 6.1.1 Security Audit Functions

The TOE provides the ability to generate audit records for all security-related auditable actions. The TOE also provides an interface to allow authorized configuration administrators and authorized audit administrators the ability to review the audit records. The Voltage SecurePolicy Suite and the IBE Gateway have separate auditing systems that are described here.

#### *6.1.1.1 Auditing functions for Voltage SecurePolicy Suite*

Security audit generation: FAU_GEN_EXP.1a, FAU_GEN_EXP.2

Audit data is generated by the following event sources within the Voltage SecurePolicy Suite:

- Web Server
- Zero Download Messenger
- Key Server
- Identity Adapters
- Server Management Console
- Policy Server

The audit data includes audit records for each of the auditable events identified in the FAU_GEN_EXP.1a security functional requirement. These audit records include the date and time of the event, the type of the event (e.g., log level), subject/user identity, and a success/failure indicator if appropriate. Audit records are stored in the MySQL database that is installed when the Voltage SecurePolicy Suite is installed. If the MySQL database storage space is exhausted, oldest records are overwritten by new records.

The Voltage SecurePolicy Suite components of the TOE associate audit records with the identity of the user or administrator that caused the event. The Zero Download Messenger includes the email address of the logged in user when logging events. Administrative events such as updating the Zero Download Messenger settings are identified by the HTTP session ID that may be traced to the administrator identity that logged in to that session.

FAU_GEN_EXP.1a has a dependency on FPT_STM.1 that specifies an underlying abstract machine system clock in the environment to provide reliable timestamps for audit events. The Voltage SecurePolicy Suite makes appropriate system calls to the respective underlying abstract machine operating systems to retrieve the time.

Security audit review: FAU_SAR_EXP.1a, FAU_SAR_EXP.3

The Server Management Console provides a web interface to allow authorized configuration administrators and authorized audit administrators the ability to review the audit trail. The interface displays all the fields of the audit records in chronological order.

The Server Management Console provides the ability for the authorized configuration administrators and authorized audit administrators to search the audit records based on the time, presumed subject identity or role, event source, log level (Error, Warning, Normal, Verbose, All), session ID, or status.

The Voltage SecurePolicy Suite relies on authentication of administrators to prevent unauthenticated (unauthorized) persons from accessing audit data.

#### *6.1.1.2 Auditing functions for Voltage IBE Gateway*

Security audit generation: FAU_GEN_EXP.1b

Audit data is generated by Voltage IBE Gateway for each of the auditable events identified in the FAU_GEN_EXP.1b security functional requirement. These audit records include the date and time of the event, the type of the event (e.g., log level), and a success/failure indicator if appropriate. Gateway audit logs are stored in flat files maintained by, and stored within the environment (OS) filesystem. If the audit record storage space is exhausted, oldest log files are overwritten by new log files.

The Voltage SecurePolicy Suite components of the TOE associate audit records with the identity of the user or administrator that caused the event.

The Voltage IBE Gateway components associate audit records with the identity of the user that caused the event. Administrators are identified by role within audit records.

FAU_GEN_EXP.1b has a dependency on FPT_STM.1 that specifies an underlying abstract machine system clock in the environment to provide reliable timestamps for audit events. The IBE Gateway makes appropriate system calls to the respective underlying abstract machine operating systems to retrieve the time.

Security audit review: FAU_SAR_EXP.1b, FAU_SAR_EXP.1c

The Voltage IBE Gateway relies on utilities in the environment (the operating system **less** command, that is invoked using the IBE Gateway command line interface) to provide the capability for authenticated administrators to view audit records. The operating system access controls prevent unauthenticated (unauthorized) persons from accessing audit data.

### 6.1.2 Communication

#### *6.1.2.1 Non-repudiation of Origin*

Selective proof of origin FCO_NRO_EXP.1

Non repudiation of origin is provided by the Voltage SecureMail plug-in component. The SecureMail plug-in component of the TOE signs every email message that is sent. When users send an encrypted email, the plug-in generates a public/private DSA key pair. The public key is sent to the Policy Server where it is signed by the server's built in certificate authority capability. The resulting X.509 certificate is returned to the Voltage SecureMail plug-in. The DSA private key is used to sign outgoing email messages and public key certificate is sent with the email message. Other SecureMail plug-in users use the public key certificate to verify the signature.

### 6.1.3 Cryptographic Support

The TOE Policy Server Key Server component provides cryptographic support for generating and managing keys and key material used for encryption and decryption of client-server communication channels and email message content.

#### *6.1.3.1 Cryptographic Support*

Cryptographic key management: FCS_CKM.1a FCS_CKM.1b, FCS_CKM_EXP.1a, FCS_CKM_EXP.1b, FCS_CKM_EXP.1c, FCS_CKM_EXP.1d, FCS_CKM.4

The Voltage SecureMail Suite TOE components generate cryptographic keys following FIPS 140 and IEEE P1363.3 methods. The TOE performs DSA signature generation and verification for non-repudiation of origin of email messages.

The TOE uses TDES encryption and decryption to provide privacy for email objects handled by the TOE. The TOE transfers the TDES email encryption key to the recipient by using IBE encryption. That is, the sender TDES-encrypts an email message and then uses the recipient's IBE public key (his globally unique email address) to encrypt the TDES key that is then sent along with the email object.

- DSA 1024-bit keys are used for signing and verifying email messages and for signing DSA public keys. DSA keys are generated by the TOE components in accordance with FIPS 186-2 *Digital Signature Standard* (DSS) with Change Notice 1 dated October 5, 2001. When their validity period expires, these keys are zeroized.

- RSA 512-2048-bit keys are used within the TLS protocol for symmetric key transfer. A configuration administrator can choose the key length using the Server Management Console. The administration documentation instructs to choose key lengths of 1024 bits or higher. The keys are generated using a FIPS approved DRNG in accordance with PKCS#1 v1.5 and PKCS#1 v.1.5 with OAEP.

- IBE 1024-bit keys are used for identity based encryption and decryption of email messages. The vendor asserts these keys are generated according to the draft IEEE P1363.3 on pairing-based cryptography. The Policy Server Key Server component generates IBE private and public keys (along with a lifetime / expiration attribute that is fixed at one week). When their validity period expires, these keys are zeroized following FIPS 140-2 key management requirements. IBE keys used for encryption or decryption by the IBE Gateway or the Zero Download Messenger are generated on demand and are zeroized after use.

- AES session keys (128 bits, 192 bits, and 256 bits) used within the TLS protocol and within the email encryption and decryption protocol are generated using a FIPS approved DRNG in accordance with FIPS 186-2 with Change Notice 1 dated October

5, 2001.

- TDES session keys used within the TLS protocol or TDES keys used for encryption and decryption of email messages are generated using a FIPS approved DRNG in accordance with FIPS 186-2 with Change Notice 1 dated October 5, 2001.

The TOE destroys cryptographic keys following FIPS 140-2 key zeroization techniques.

Cryptographic operations: FCS_COP.1a, FCS_COP.1b, FCS_COP.1c, FCS_COP.1d, FCS_COP.1e, FCS_COP_EXP.1

The TOE performs TDES encryption and decryption for the privacy of email objects in accordance with FIPS Publication 46-3, *Data Encryption Standard.* Compliance was verified using the tests found in NIST Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*. This testing is performed by NVLAP accredited Cryptographic Module Testing (CMT) laboratories. (See FIPS Triple-DES validation certificate 291.)

The TOE performs TDES and AES encryption and decryption within the TLS protocol in accordance with FIPS Publication 46-3, *Data Encryption Standard* and FIPS Publication 197, *Advanced Encryption Standard,* respectively. TDES compliance was verified using the tests found in NIST Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*. AES compliance was verified using the tests found in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). This testing is performed by NVLAP accredited Cryptographic Module Testing (CMT) laboratories. (See FIPS Triple-DES validation certificate 291, and AES validation certificate 199.)

The TOE performs IBE encryption and decryption of symmetric keys for the purpose of symmetric key exchange within the IBE protocol in accordance with draft P1363.3 on pairing-based cryptography.

The Voltage SecureMail plug-in [FCS_COP_EXP.1] performs DSA signature generation and verification and the TOE performs DSA encryption and decryption of symmetric keys for the purpose of key exchange within the TLS protocol. DSA cryptographic operations are in accordance with FIPS 186-2, *Digital Signature Standard* (DSS). DSA algorithm compliance was verified using tests described in *Digital Signature Algorithm Validation System (DSAVS).* Note that this is a new document containing validation tests that relate to FIPS 186-2 with Change Notice 1 dated October 5, 2001. The testing is handled by NVLAP-accredited Cryptographic Module Testing (CMT) laboratories. (See FIPS DSA validation certificate 124.)

### 6.1.4 Identification and Authentication

The TOE identification and authentication capabilities ensure that TOE users are associated with the proper security attributes (e.g. identity, groups, and roles).

User Identification and authentication: FIA_UID_EXP.2a, FIA_UID_EXP.2b, FIA_UID_EXP.2c, FIA_UID_EXP.2d, FIA_UID_EXP.2e, FIA_UAU_EXP.2a, FIA_UAU_EXP.2b, FIA_UAU_EXP.2c, FIA_UAU_EXP.2d, FIA_UAU_EXP.2e.

All TOE-user interactions require identification and authentication before allowing any TSF-mediated actions:

- The Zero Download Messenger uses the question and answer or email answerback identity adapter to initially authenticate users. Users must respond by answering questions, one of which requires entering a correct password that is at least 8 characters in length and includes at least one of the following: capital letters, lowercase letters, numbers, and punctuation. Once a session has closed, this password must be presented to the question and answer identity adapter for subsequent reauthentication. Identification and authentication credentials used by the Zero Download Messenger are used within the Voltage SecurePolicy Suite.

- Voltage SecureMail plug-in users authenticate to their Windows Domain by entering their username and password. On success, the domain returns Windows domain credentials to confirm user authentication status for subsequent operations. The Voltage SecureMail plug-in for Outlook cannot start unless Microsoft Outlook starts. On startup, Microsoft Outlook checks for valid Windows domain credentials before starting up. In the case where a Voltage SecureMail plug-in for Outlook is in a domain not supported by the Active directory (for example, an external domain), that domain authentication method is used. When that client attempts to obtain a private IBE key, the established Voltage SecurePolicy Suite Authentication adapter authenticates the user using an Email Answerback or Question and Answer protocol as applicable.

- The IBE Gateway CLI may be started only by an IT administrator who is logged into the environment. A gateway administrator must log into the environment using the gateway administrator account name and password before any administrative TOE security functions are provided by the IBE Gateway.

- Voltage SecurePolicy Suite administrators authenticate to their Windows Domain by entering their username and password. On success, the domain returns Windows domain credentials to confirm user authentication status for subsequent operations The Voltage SecurePolicy Suite confirms administrators and users are authenticated before providing any services via the administration GUI. The Voltage SecurePolicy Suite interacts with Active Directory to determine user authentication status within the Windows domain before providing any TOE services.

### 6.1.5 Security Management

The TOE allows management of TSF data and security attributes relying on roles implemented by the TOE and the IT environment to control access to these management functions.

Management of security attributes: FMT_MSA.1, FMT_MSA.2, FMT_SMF.1, and FMT_SMR.1

FCS_CKM.1 and FCS CKM.4 have a dependency on FMT_MSA.2 to ensure that security attributes are secure. The security attributes (in this case, symmetric and asymmetric keys generated for various cryptographic functions) are generated and destroyed according to specific standards that ensure they are secure attributes. Both key generation and destruction comply with FIPS 140-2 Level 1 key management requirements of FIPS 140-2.

FMT_MSA.2 has a dependency on FMT_MSA.1 to restrict the ability to modify security attributes (cryptographic keys). In this case the TSF environment for the client hosting the Voltage SecureMail plug-in uses the operating system access controls to prevent unauthorized access to keys stored in the Encrypting File System. Only authenticated users may access these security attributes.

FMT_MSA.1 also has a dependency on FDP_ACC.1 to enforce access controls as a means to regulate access to TOE security functions. This Security Target considers user data to be cryptographic keys stored in encrypted form in the environment (on the Voltage SecureMail plug-in client) or email objects encrypted or decrypted by TOE security functions. The three TOE subsystems (the Voltage SecurePolicy Suite, Voltage SecureMail plug-in client and the IBE Gateway) implement access control subsystems in their respective environments that provide the required access control mechanisms.

FMT_MSA.1 has a dependency on FMT_SMF.1 to provide security attribute management functions. The IT environment for three TOE subsystems (the Voltage SecurePolicy Suite, Voltage SecureMail plug-in client and the IBE Gateway) provide specific access control utilities for use by IT administrators in managing user and group membership and to manage permissions based on user name and group membership.

FMT_MSA.1 also has a dependency on FMT_SMR_EXP.1a, FMT_SMR_EXP.1b, and FMT_SMR_EXP.1c to maintain security roles for use in managing access. The Voltage SecureMail plug-in for Outlook maintain the user role for associating an individual user (the authenticated user) with TSF-relevant operations. These operations consist of IBE and DSA key management and use. The Voltage SecurePolicy Suite maintains the configuration administrator and audit administrator roles for controlling access to TOE security functions. The Voltage IBE Gateway maintains the administrator role for controlling access to TOE security functions.

FMT_SMR.1 specifies the IT administrator role (for the IT environment) to regulate who may modify the security attributes group membership and file permissions maintained in the IT environment.

### FMT_MTD_EXP.1a and FMT_MTD_EXP.1b Management of TSF data

The Voltage SecurePolicy Suite stores TSF data identified in Table 4 and limits the capability to modify this data to the authorized configuration administrator. The Voltage IBE Gateway stores TSF data identified in Table 5 and limits the capability to modify this data to the authorized configuration administrator.

FMT_MTD_EXP.1a and FMT_MTD_EXP.1b have a dependency on FMT_SMF.1 to provide security attribute management functions using the Voltage SecurePolicy Suite administration interface of the TOE and the IBE Gateway CLI. These interfaces allow respective authorized administrators to manage the TSF data identified in Table 6 (for Voltage SecurePolicy Suite) and Table 7 (for the IBE Gateway).

FMT_MTD_EXP.1 has a dependency on FMT SMR_EXP.1a and FMT SMR_EXP.1b to maintain security roles for use in managing access. The Voltage SecurePolicy Suite maintains the roles configuration administrator and audit administrator to regulate access. The IBE Gateway supports a single administrator role, associating administrative users with this role.

### 6.1.6 Protection of the TSF

Basic internal TSF data transfer protection: FPT_ITT.1

The TOE uses the TLS protocol to transfer sensitive data between TOE components residing on the same machine. That is, the TOE includes TLS client and server components that pass data (private and public keys) between the policy server and Zero Download Messenger.

Inter-TSF confidentiality during transmission: FPT_ITC.1

The TOE uses the TLS protocol to transfer sensitive data between the TOE and a remote trusted IT product. That is TLS is used to pass data (private keys) between the following components:

- the policy server and Voltage SecureMail plug-in for Outlook
- the policy server and IBE Gateway
- the Zero Download Messenger and a browser capable of using the TLS protocol

Non-bypassability of the TSP: FPT_RVM_EXP.1a, FPT_RVM_EXP.1b

TSF management functions are protected by requiring identification and authentication before allowing access. I&A functions must succeed before management functions may proceed.

The IT environment also supports non-bypassability by ensuring that subjects cannot bypass the environment security functions.

Domain separation: FPT_SEP_EXP.1a, FPT_SEP_EXP.1b

The TOE establishes a security domain for its own execution through the correct programmatic use of memory management techniques and OS security capabilities. The TSF requires administrators and users to be properly identified and authenticated before they may access security functions. Physical security assumptions and other personnel assumptions help protect the TOE from physical and logical tampering.

## 6.2 Security Assurance Measures

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

| Assurance Requirement | Assurance Components |
|---|---|
| ACM_CAP.2 | The description of the configuration items is provided in ACM_CAP.2. |
| ADO_DEL.1 | The description of the delivery procedures is provided in ADO_DEL.1 and the following documents.<br>• Customer Letter<br>• CustomerLetterAttachmentV0.1.doc |
| ADO_IGS.1 | The installation, generation, and start-up procedures are provided in :<br>• *Read Me First for Installers Voltage SecureMail Suite 2.0 Common Criteria Supplemental Guidance*<br>• *Voltage SecurePolicy Suite 2.0 Administrators Guide*<br>• *Voltage SecurePolicy Suite 2.0 Installation Guide For Windows*<br>• *Voltage IBE Gateway Server 2.0 Installation and Upgrade Instructions*<br>• *Voltage IBE Gateway Server 2.0 Setup Guide*<br>• *Voltage IBE Gateway Server 2.0 Configuration Guide*<br>• *Voltage SecurePolicy Server 2.0 Release Notes*<br>• *Voltage IBE Gateway Server 2.0 Release Notes* |
| ADV_FSP.1 | The informal functional specification is provided in *EAL2 Design Documentation Voltage SecureMail Suite 2.0*. |
| ADV_HLD.1 | The descriptive high-level design is provided in *EAL2 Design Documentation Voltage SecureMail Suite 2.0*. |
| ADV_RCR.1 | The informal correspondence demonstration is provided in *EAL2 Design Documentation Voltage SecureMail Suite 2.0*. |
| AGD_ADM.1 | The administrator guidance is provided in the following documents:<br>• *Read Me First for Administrators Voltage SecureMail Suite 2.0 Common Criteria Supplemental Guidance*<br>• *Voltage SecurePolicy Suite 2.0 Administrators Guide*<br>• *Voltage IBE Gateway 2.0 Configuration Guide* |

| Assurance Requirement | Assurance Components |
|---|---|
| AGD_USR.1 | The user guidance is provided in the following documents:<br>• *Read Me First for Users Voltage SecureMail Suite 2.0 Common Criteria Supplemental Guidance* |
| ATE_COV.1 | The evidence of coverage is provided in <title>. |
| ATE_FUN.1 | The functional testing description is provided in <title>. |
| ATE_IND.2 | The TOE and testing documentation were made available to the CC testing laboratory for independent testing. |
| AVA_SOF.1 | The strength of TOE security function analysis is provided in *EAL2 Strength of TOE Security Function Analysis Voltage SecureMail Suite 2.0*. |
| AVA_VLA.1 | The vulnerability analysis performed is provided in *EAL2 Vulnerability Analysis Voltage SecureMail Suite 2.0*. |

**Table 13 - Assurance Requirements: EAL2**

## 6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 2.4.

| | Audit | Communication | Cryptographic Operation | Identification & Authentication | Security Management | Protection of TOE functions |
|---|---|---|---|---|---|---|
| FAU_GEN_EXP.1a | X | | | | | |
| FAU_GEN_EXP.1b | X | | | | | |
| FAU_GEN_EXP.2 | X | | | | | |
| FAU_SAR_EXP.1a | X | | | | | |
| FAU_SAR_EXP.1c | X | | | | | |
| FAU_SAR_EXP.3 | X | | | | | |
| FCO_NRO_EXP.1 | | X | | | | |
| FCS_CKM.1a | | | X | | | |
| FCS_CKM.1b | | | X | | | |
| FCS_CKM_EXP.1a | | | X | | | |
| FCS_CKM_EXP.1b | | | X | | | |
| FCS_CKM_EXP.1c | | | X | | | |
| FCS_CKM_EXP.1d | | | X | | | |
| FCS_CKM.4 | | | X | | | |
| FCS_COP.1a | | | X | | | |
| FCS_COP.1b | | | X | | | |
| FCS_COP.1c | | | X | | | |

| | Audit | Communication | Cryptographic Operation | Identification & Authentication | Security Management | Protection of TOE functions |
|---|---|---|---|---|---|---|
| FCS_COP.1d | | | X | | | |
| FCS_COP.1e | | | X | | | |
| FCS_COP_EXP.1 | | | X | | | |
| FIA_UID_EXP.2a | | | | X | | |
| FIA_UID_EXP.2d | | | | X | | |
| FIA_UID_EXP.2e | | | | X | | |
| FIA_UAU_EXP.2a | | | | X | | |
| FIA_UAU_EXP.2d | | | | X | | |
| FIA_UAU_EXP.2e | | | | X | | |
| FMT_MSA.2 | | | | | X | |
| FMT_MTD_EXP.1a | | | | | X | |
| FMT_MTD_EXP.1b | | | | | X | |
| FMT_SMR_EXP.1a | | | | | X | |
| FMT_SMR_EXP.1b | | | | | X | |
| FMT_SMR_EXP.1c | | | | | X | |
| FPT_ITC.1 | | | | | | X |
| FPT_ITT.1 | | | | | | X |
| FPT_RVM_EXP.1a | | | | | | X |
| FPT_SEP_EXP.1a | | | | | | X |

**Table 14 – TOE Security Function to SFR Mapping**

## 6.4 Appropriate Strength of Function Claim

The claim of SOF-basic for the Identification and Authentication security function is consistent with the claim of SOF-Basic for FIA_UAU_EXP.2e and FIA_UID_EXP.2e SFRs that map to that security function.

## 6.5 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

| Assurance Requirement | Assurance Measures | Assurance Rationale |
|---|---|---|
| ACM_CAP.2 | Configuration Items | The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE. |
| ADO_DEL.1 | Delivery Procedures | The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer. |
| ADO_IGS.1 | Installation generation and startup procedures | The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE. |
| ADV_FSP.1 | Informal Functional Specification | The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces. |
| ADV_HLD.1 | Descriptive High Level Design Documentation | The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified. |
| ADV_RCR.1 | Informal Correspondence Demonstration | The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD. |

| Assurance Requirement | Assurance Measures | Assurance Rationale |
|---|---|---|
| AGD_ADM.1 | Administrator Guidance | The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items. |
| AGD_USR.1 | User Guidance | The user guidance describes the security functions and interfaces in a way that allows a user to interact with the TOE securely. |
| ATE_COV.1 | Evidence of coverage | The test coverage document provides a mapping of the test cases performed against the TSF. |
| ATE_FUN.1 | Functional testing | The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort. |
| ATE_IND.2 | Independent testing - sample | The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing. |
| AVA_SOF.1 | Strength of TOE security function evaluation | The Strength of TOE security function evaluation document shows how a TOE probabilistic or permutational security mechanism meets or exceeds the minimum strength level defined in the ST. |
| AVA_VLA.1 | Developer vulnerability analysis | The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability. |

**Table 15 – Assurance Measure Rationales**

# 7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

# 8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

## 8.1 Security Objectives Rationale

Sections 4.3 - 4.6 provide the security objectives rationale.

## 8.2 Security Requirements Rationale

Sections 5.7 - 5.12 provide the security requirements rationale.

## 8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification rationale.

## 8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.