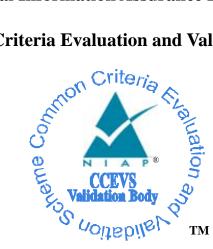# National Information Assurance Partnership

## Common Criteria Evaluation and Validation Scheme



™

## Validation Report

# Voltage Security, Inc.
# Palo Alto, CA

## Voltage SecureMail Suite 2.0

**Report Number:**     **CCEVS-VR-07-0029**
**Dated:**             **29 May 2007**
**Version:**          **1.3**

# Table of Contents

# 1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR) which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Voltage SecureMail Suite 2.0, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the Voltage SecureMail Suite 2.0 product was performed by InfoGard Laboratories, Inc., San Luis Obispo, CA in the United States and was completed on February 19, 2007. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 2 (EAL2) - augmented, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2.

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.

Configuration I of the TOE 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 is 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 with 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.
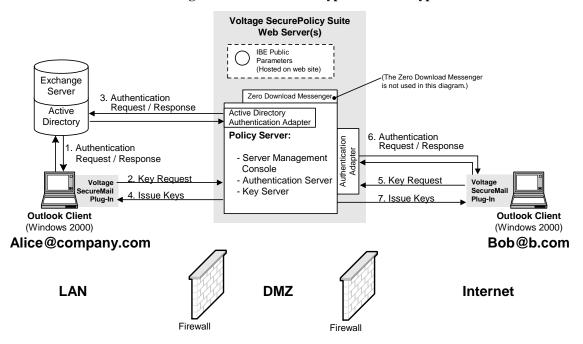
**Figure 1 End-to-End Encryption and Decryption**



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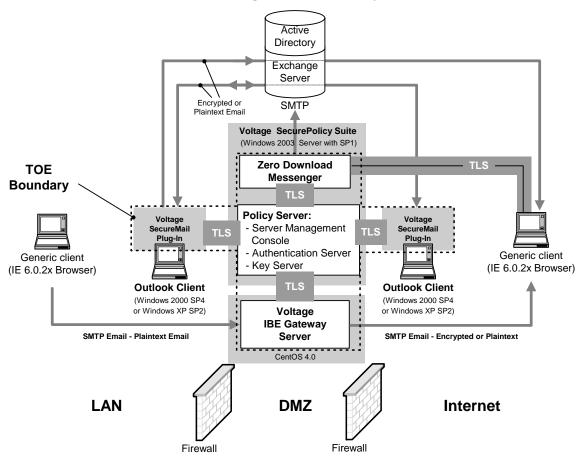
Additional TOE functionality is provided by the Zero Download Messenger. TOE Configuration II adds the Voltage IBE Gateway Server to TOE Configuration I.

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.

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**



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.

The following components are present in the Voltage SecureMail Suite but are were not evaluated (excluded from the Common Criteria Evaluated Configuration):

- 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.

# 2  Identification of the TOE

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL pay a fee for their product's NIAP Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

| Evaluation Scheme | United States Common Criteria Evaluation Validation Scheme |
|---|---|
| Evaluated Target of Evaluation | Voltage SecureMail Suite 2.0 |
| Protection Profile | Not applicable |
| Security Target | Voltage SecureMail Suite 2.0 Version 1.18 May 4, 2007 |
| Dates of evaluation | Start Date: 10/13/05 Finish Date: 2/19/07 |
| Conformance result | Part 2 extended, Part 3 conformant, EAL 2 |
| Common Criteria version | CC version 2.2 |
| Common Evaluation Methodology (CEM) version | CEM version 2.2 |
| Evaluation Technical Report (ETR) | 07-797-R-0035 V1.1 |
| Sponsor/Developer | Voltage Security 1070 Arastadero Road, Suite 100 Palo Alto, CA 94304 |
| Common Criteria Testing Lab (CCTL) | InfoGard Laboratories |
| CCTL Evaluators | Mark Plascencia, Albert Chang |
| CCEVS Validators | Deborah Downs, Aerospace Corporation Nicole Carlson, Aerospace Corporation |

# 3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before 10/13/05.

# 4 Security Policy

The Voltage SecureMail Suite 2.0 performs the following security functionality:

## 4.1 Audit

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

### 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: Time Presumed subject identity or role Event source Log level (Error, Warning, Normal, Verbose, All) Session ID Status |

### 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 less to review audit messages. |

## 4.2 Communication

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

## 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. |

## 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 |

## 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. |

## 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. |

# 5  Assumptions

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

## 5.1  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

## 5.2  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.

## 5.3 Operational Security 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.

# 6 Evaluated configuration

The evaluated configuration consists of the following 2 options, both of which require software and hardware deployed to be in the evaluated configuration of the TOE:

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

The TOE (Configuration I) consists of a **Voltage SecurePolicy Suite**, and a **Voltage SecureMail plug-in for Microsoft Outlook**.

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.

TOE Configuration II adds the Voltage IBE Gateway Server to TOE Configuration I.

## 6.1 Architectural Information

The high-level architecture of the TOE is shown in Figure 2.

## 6.2  TOE Hardware

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** **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). |

| TOE or Environment | Component | Description |
|---|---|---|
| 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 1 Hardware Components**

## 6.3  TOE Software

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 2 Software Components**

# 7 Documentation

The following documentation is delivered with the TOE:

- Read Me First for Installers Voltage SecureMail Suite 2.0 Common Criteria Supplemental Guidance

- Voltage SecurePolicy Suite 2.0 Administrators Guide

- Voltage SecurePolicy Suite 2.0 Installation Guide For Windows

- Voltage IBE Gateway Server 2.0 Installation and Upgrade Instructions

- Voltage IBE Gateway Server 2.0 Setup Guide

- Voltage IBE Gateway Server 2.0 Configuration Guide

- Voltage SecurePolicy Server 2.0 Release Notes

- Voltage IBE Gateway Server 2.0 Release Notes
- Read Me First for Users Voltage SecureMail Suite 2.0 Common Criteria Supplemental Guidance

- 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

# 8 IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

## 8.1 Developer testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. During the evaluation of the ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The evaluation team reviewed the Developer's test plan and assessed that all security functions were tested except the following:

- Cryptographic key generation - FCS_CKM.1a, FCS_CKM.1b

- Cryptographic key destruction - FCS_CKM.4

- Cryptographic operations - FCS_COP.1a, FCS_COP.1b, FCS_COP.1c, FCS_COP.1d, FCS_COP.1e

The evaluation generated additional tests during Independent Testing to test the security functions that were not tested by the Developer's test plan.

## 8.2 Evaluation Team Independent Testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features

- Security functions critical to the TOE's security objectives

- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation

- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team reran 30% of the Sponsor's test cases and specified additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

## 8.3 Vulnerability Analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Strength of Function analysis, the Developer Vulnerability Analysis, and the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of six (6) penetration tests.

# 9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

InfoGard Laboratories has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in February 2007.

# 10 Validator Comments/Recommendations

The TOE makes use of cryptographic modules in order to fulfill some security functions. Cryptographic modules are evaluated under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2, a separate standard from the Common Criteria; the cryptographic functions were not evaluated further during this evaluation. Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate.

# 11 Security Target

Voltage SecureMail Suite 2.0 Version 1.18 May 4, 2007

# 12 Bibliography

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.2, January 2004. CCIMB-2004-01-001.

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.2, January 2004. CCIMB-2004-01-002.

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.2, January 2004. CCIMB-2004-01-003.

Common Criteria Project Sponsoring Organisations. Common Criteria Commmon Methodology for Information Technolgoy Security Evaluation. January 2004 CCIMB-2004-01-004.

Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

Voltage SecureMail Suite 2.0 Version 1.18 May 4, 2007