National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1

Report Number: CCEVS-VR-VID10003-2008
Dated: December 18, 2008
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Mr. Daniel P. Faigin
The Aerospace Corporation
El Segundo, California

Ms. Jandria S. Alexander
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Mr. Clifton Morgan
Mr. Sai Pulugurtha
CygnaCom Solutions
McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1 Security Target.

Table of Contents

List of Figures

List of Tables

1.0 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The GuardianEdge Platform provides transparent encryption services for hard disks and removable storage devices on computers running Windows XP. It employs full disk encryption, pre-boot authentication, and on-the-fly disk decryption/encryption at the device driver level to provide complete protection of data on Windows-based notebook and desktop systems. It also protects information on removable storage devices such as USB flash drives.

The GuardianEdge Platform is intended for use in computing environments where there is a potential for attackers possessing a moderate attack potential.

The GuardianEdge Platform protects data at rest on the hard disk and on removable devices from unauthorized access. The GuardianEdge Platform uses its own FIPS 140-2 validated cryptographic library to perform the cryptographic operations necessary to protect data, support authentication, and self-protect itself against tampering or bypass. The product uses Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with 256-bit keys to perform bulk encryption on administrator-specified partitions of hard disks and removable storage devices on a Client Computer.

The Guardian Edge Platform uses a mix of FIPS-validated and non-validated algorithms. Those algorithms that have undergone FIPS evaluation are as follows:

- AES (Certs. #154 and #759)
- HMAC (Cert. #414)
- SHS (Certs. #239 and #766)
- RNG (Certs. #45 and #437)

The HMAC-SHA-1 algorithm has a certificate (SHS Cert. #239), but is vendor-affirmed. The Elliptical Curve Cryptographic Algorithm used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. This algorithm has only been asserted as tested by the vendor.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in November 2008. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.3 from the Common Methodology for Information Technology Security Evaluation, Version 2.3, [CEM]. The product is not

conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1.

2.0 Identification

Target of Evaluation:	GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1
Evaluated Software:	GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1
Developer:	475 Brannan Street, Suite 400, San Francisco CA 94107-5421
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Evaluators:	Clifton Morgan, Sai Pulugurtha
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Daniel Faigin, Jandria Alexander
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005

3.0 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

3.1 Security Audit

The TOE auditing service generates audit records into the Windows system event log of the Client Computer operating system. It captures security events related to use of the authentication mechanism, initial encryption activity, and the startup and shutdown of the TOE client. The TOE auditing service is automatically started with the start-up of the TOE client, and there is no interface to turn off the audit mechanism and no interface to change the security events being audited.

The audit function requires the following support from the TOE's IT environment:

- The OS to protect the Windows system event log to ensure it's protected from unauthorized deletion and modification.
- The platform to provide reliable time when required to ensure the audit records have meaningful timestamps.
- The OS to provide an interface to view the audit records in the Windows system event log.

3.2 Data Protection

The TOE uses its FIPS140-2 cryptographic functions, described below, to ensure all data on the hard disk partitions, as designated by an administrator, is protected by encryption when not in use (i.e., at rest). Except for the GEFS files (to bootstrap the system), the encryption covers all the data on the selected hard disk partitions, including system files, e.g., Windows operating system files, registry, swap files, hibernation files, paging files. A per computer key is used to encrypt all data on the hard disk; this key is called the Workstation Encryption Key (WEK).

The data protection function also ensures the data is available when requested and that both the encryption process (to protect the data when at rest) and the decryption process (to make the data available to registered users) is done transparently to the user, referred to as on-the-fly decryption/encryption. This transparent operation ensures enforcement and doesn't rely on users activating the function.

Data on removable storage devices is encrypted on a per file basis. Files are automatically encrypted when written to the device. Encrypted files are decrypted when accessed and encrypted when written. Depending on the configuration, pre-existing plaintext files may be either automatically encrypted, or left as plaintext. The evaluated configuration is for pre-

existing files to be left in plaintext. A per file key is used to encrypt files on removable storage devices; this key is called the File Encryption Key (FEK).

The data protection function requires the platform to be operating correctly, both in general for supporting the TOE processes and in particular for loading the TOE kernel-mode device drivers as configured in the installation process and processing the bits to ensure they pass through the TOE for the specified partitions.

3.3 Cryptographic Services

The TOE includes cryptographic libraries that provide cryptographic support for the following security functions:

- Authentication process password check
  - Elliptic Curve Cryptography (ECC)
  - SHA-1
- New user registration
  - ECC
  - RNG
- Initial encryption and transparent decryption: AES in CBC mode.
- Self-tests and integrity checks: SHA-1 and CRC.

The IT environment is only required to operate correctly to support the cryptographic services security function.

Cryptographic Algorithms Certifications are as follows:

- AES (Certs. #154 and #759);
- HMAC-SHA-1 (SHS Cert. #239, vendor affirmed);
- HMAC (Cert. #414);
- SHS (Certs. #239 and #766);
- RNG (Certs. #45 and #437); and
- Elliptical Curve Cryptographic Algorithm (verified by Vendor Assertion).

3.4 Identification and Authentication

The TOE provides an identification and authentication (I&A) mechanism that requires all users to identify and authenticate themselves during the startup of the Client Computer, before the operating system is loaded and before users log on to their Windows accounts. This is referred to

as pre-Windows authentication. In addition to the pre-Windows authentication requirement, the TOE also requires all users to log on again when accessing the GuardianEdge Client console.

Supporting the password-based mechanism, the TOE obscures the password users enter on the TOE logon screens. It provides an authentication failure mechanism and password management options that defines parameters for acceptable passwords.

The identification and authentication function depends on the operating system to identify and authenticate the Client Computer users after startup, and the platform to provide an accurate clock to measure one minute, the delay in the logon process for the authentication failure mechanism. As with all the security functions, it also requires the support provided as part of the Partial Self-Protection, described below, both in general and in particular for activating the TOE as part of the pre-Windows start-up process.

3.5 Security Management

The TOE includes an administrative interface for Client Administrators to remove users, change passwords, and perform initial encryption on selected partitions. Registered users also use this interface to change their passwords. The GuardianEdge Platform in its evaluated configuration is designed to require minimum administration during normal operation. The Client Administrator, using the Client Console, is also able to verify the evaluated configuration settings. New users are added to the TOE through a self-registration process coordinated with the operating system logon for subsequent users after startup of the Client Computer.

The IT environment is required to operate correctly to support this security function.

3.6 Partial Self-Protection

Working in concert with its platform the TOE provides a security architecture and security mechanisms to ensure the TSF cannot be bypassed, corrupted, or otherwise compromised.

The TOE relies on its platform for domain separation of TSF processes, for non-bypassability, for access controls on file protections, and for correct operation of the BIOS and media driver data processing.

3.7 Access Banner

The TOE displays an advisory warning access banner as part of its logon screen. The banner and warning are defined by the Policy Administrator during the installation process.

3.8 Summary

A summary of the SFRs for the TOE and IT environment are included in the following tables. Note that _EXP in the SFR ID indicates explicitly specified requirements.

Table 1. TOE Security Functional Requirements

Item	SFR ID	SFR Title
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User Identity Association
3.	FCS_CKM.1	Cryptographic key generation
4.	FCS_CKM.4	Cryptographic key destruction
5.	FCS_COP.1(1)	Cryptographic Operation (AES)
6.	FCS_COP.1(2)	Cryptographic Operation (ECC of UPC)
7.	FCS_COP.1(3)	Cryptographic Operation (RNG)
8.	FCS_COP.1(4)	Cryptographic Operation (Secure Hash)
9.	FCS_COP.1(5)	Cryptographic Operation (HMAC-SHA-1)
10.	FDP_IFC.2	Complete information flow control
11.	FDP_IFF.1	Simple security attributes
12.	FIA_AFL.1	Authentication failure handling
13.	FIA_SOS.1	Verification of secrets
14.	FIA_UAU.2	User authentication before any action (user access to Client Computer)
15.	FIA_UAU_TOE_EXP.2	User authentication before any action (Client console)
16.	FIA_UAU.7	Protected authentication feedback
17.	FIA_UID.2	User identification before any action (user access to Client Computer)
18.	FIA_UID_TOE_EXP.2	User identification before any action (Client console)
19.	FMT_MSA.1	Management of security attributes
20.	FMT_MSA.2	Secure security attributes
21.	FMT_MSA.3	Static attribute initialization
22.	FMT_MOF.1	Management of security functions behaviour
23.	FMT_MTD.1	Management of TSF data
24.	FMT_SMF.1	Specification of Management Functions
25.	FMT_SMR.1	Security roles
26.	FPT_RVM.1(1)	Non-bypassability of the TSP (TOE)
27.	FPT_SEP_TOE_EXP.1	TSF partial domain separation

Item	SFR ID	SFR Title
28.	FPT_TST.1	TSF testing
29.	FTA_TAB.1	Default TOE access banners

Table 2. IT Environment Security Functional Requirements

Item	SFR ID[1]	SFR Title
30.	FAU_SAR.1	Audit review
31.	FAU_STG.1	Protected audit trail storage
32.	FIA_UAU_ENV_EXP.2	User authentication before any action (Client Computer O/S)
33.	FIA_UID_ENV_EXP.2	User identification before any action (Client Computer O/S)
34.	FPT_AMT.1	Abstract machine testing
35.	FPT_RVM.1(2)	Non-bypassability of the TSP (Platform)
36.	FPT_SEP_ENV_EXP.1	TSF Environment partial domain separation
37.	FPT_STM.1	Reliable time stamps

[1] Note: Although these SFRs have CC tags, all of the cited SFRs have been modified to apply to the IT environment.

4.0 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL 4 augmented with ALC_FLR.3 assurance requirements.

ADO_DEL.1 Delivery procedures:

- Download Procedures are located on GuardianEdge.com

ADO_IGS.1 Installation, generation, and start-up procedures:

- GuardianEdge Hard Disk Encryption Installation Guide V9.0
- GuardianEdge Removable Storage Encryption Installation Guide V3.0
- GuardianEdge Common Criteria Supplement V1.2

AGD_ADM.1 Administrator guidance:

- GuardianEdge Hard Disk Encryption Client Administrator Guide V9.0
- GuardianEdge Removable Storage Encryption Client Administrator Guide V3.0

AGD_USR.1 User guidance:

- GuardianEdge Hard Disk Encryption User Guide V9.0
- GuardianEdge Removable Storage Encryption User Guide V3.0

4.2 Environmental Assumptions

The following assumptions apply to the security environment in which the TOE operates:

- Remote users are required to log on to the Windows operating system to gain access to the Client Computer. Therefore, Network Sharing Services that do not require a Windows Logon Authentication must be disabled.
- Administrators must be appropriately trained and follow all administrator guidance.
- All software, firmware, or hardware must be approved by the security officer.
- Users do not leave the GuardianEdge Client Computer unattended when they are logged on.
- Users will protect their authentication data.
- Client Computer users should not be given administrator privileges.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 augmented with ALC_FLR.3 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 4 augmented with ALC_FLR.3 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The TOE depends on the IT environment to provide the capability to read the audit records, protect audit information, user identification and authentication before action, run a suite of tests, reliable time stamps, non-bypassability, and TSF domain separation.
5. The following product capabilities were not covered by the evaluation:
    - GuardianEdge Server was not installed
    - Client Monitor was disabled.
    - Authenti-Check was disabled
    - One-Time Password was disabled.
    - I&A optional mechanisms:
        - Single Sign-On is disabled.
        - Token authentication ("Advanced Authentication") is disabled.
        - Autologon is disabled.
        - Grace restarts were disabled (set to zero).
    - Initial Encryption configuration:
        - Manual encrypt or decrypt partition enabled for Client Administrator only, not registered users.
        - Unused sectors are included in the encryption.
    - Removable Storage configuration:

- GuardianEdge Hard Disk Encryption is installed and all hard disk partitions of the protected operating system and associated user data partitions and swap partitions are encrypted.
- The GuardianEdge Removable Storage Access Utility is not used.
- Encryption policy set to “Encrypt New Files”.
- The option to automatically encrypt pre-existing plaintext on removable devices is disabled.
- The creation of self-extracting files is disabled.
- Non-registered user support is disabled.
- The access policy is set to read and write.
- Encryption method is set to “password.”
- Certificate (token and software based) encryption is disabled and/or not used.
- Group Key feature is disabled.
- No Master Certificate specified.

- A logon delay was set to one minute after one incorrect logon.

6. The Elliptical Curve Cryptographic (ECC) Algorithm meets the IEEE-P1363 by Vendor Assertion. There is no FIPS test vector for the ECC algorithm.
7. The encryption certificates for the product, certificate #515, only applies, with respect to XP, to SP2 (as SP3 had not been released as of the time of certification).

The ST provides additional information on the assumptions made and the threats countered.

5.0 Architectural Information

The evaluated configuration of the GuardianEdge Platform consists the software components listed below. The TOE includes all product components; however, in the evaluated configuration, some components do not provide any security functions and are therefore outside the scope of some assurance evaluation activities.

The following TOE components provide security functions in the evaluated configuration:

- **GuardianEdge Pre-Boot Authentication** operates in the pre-Windows environment to provide pre-Windows authentication, decryption services to start the operating system, self-tests, a master boot record to interface with the BIOS, and a file storage mechanism to support these functions, referred to as the GuardianEdge File System (GEFS).
- **GuardianEdge Hard Disk Encryption** includes a kernel-mode driver that performs on-the-fly decryption and encryption of data on the client hard disk.
- **GuardianEdge Removable Storage Encryption** includes a kernel-mode driver that performs decryption and encryption of data on the removable storage devices, and provides per-file password-based access control as required to decrypt files accessed on devices.
- **GuardianEdge Data Protection Framework** provides the cryptographic library and Client Console interface.

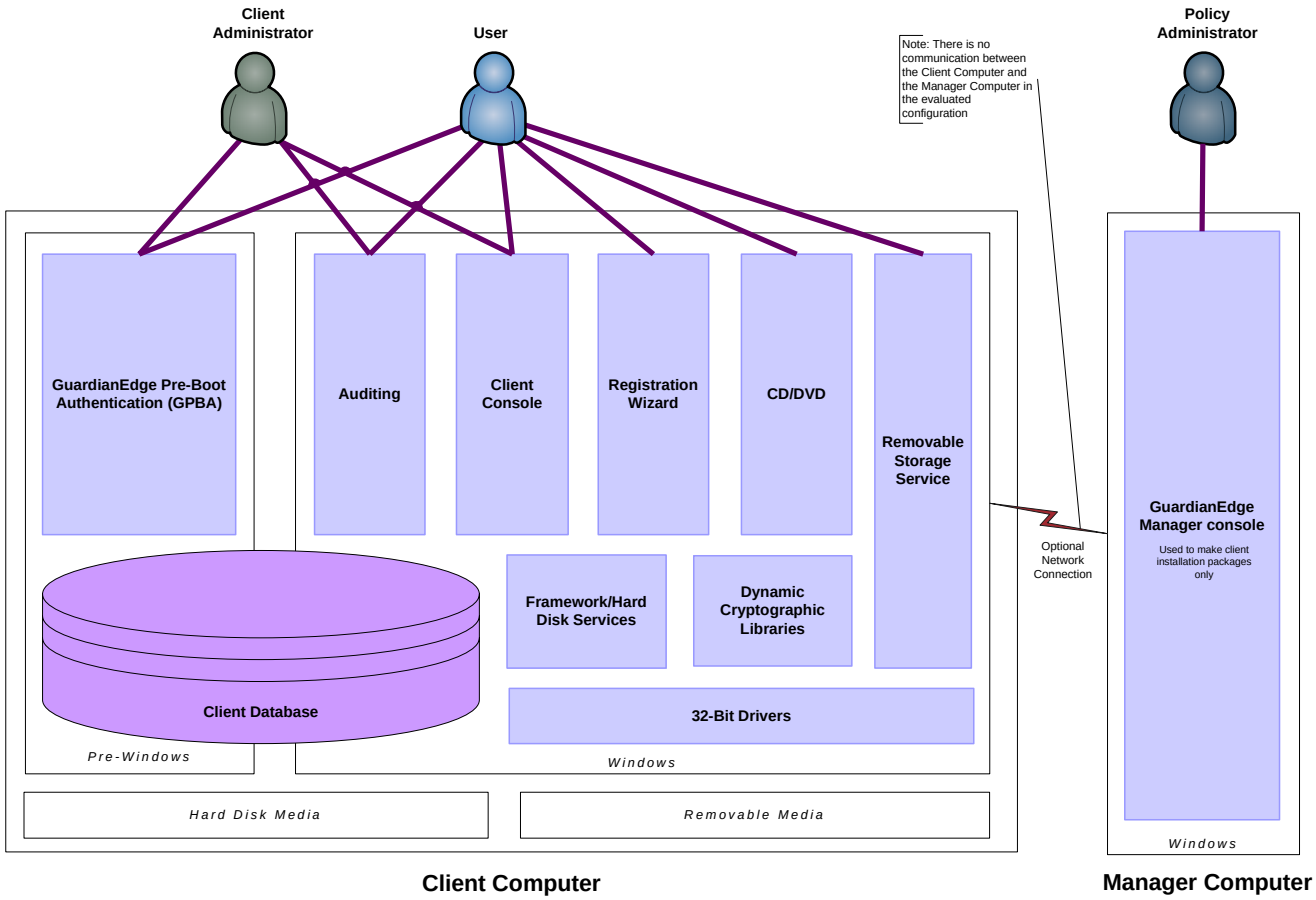

Figure 1. GuardianEdge Components and TOE Boundary

The TOE relies on the following IT environment components to support the evaluated security functions:

- The Client Computer including Windows XP Service Pack 3, x86 platform, hard disk and removable storage components and device drivers
- The Manager Computer including Windows 2003 Server Service Pack 2, x86 platform with storage media for the client installation package files.

6.0 Documentation

CC Evaluation Evidence:

Note: Bolded documents are available for GuardianEdge customers.

Table 3. Evaluation Documentation and Evidence

Acronym	Document Title
FSP	GuardianEdge Data Protection Framework 9.0.1, GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1 Functional Specification, V2.5, June 27, 2008
HLD	GuardianEdge Data Protection Framework 9.0.0 with GuardianEdge Hard Disk Encryption 9.0.0 and GuardianEdge Removable Storage Encryption 3.0.0 High-Level Design version 3.3, April 1, 2008
TAT	GuardianEdge Data Protection Framework 9.0.1, GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1 Tools and Techniques Version 3.0, April 30, 2008
LLD	LLD-0409\LLD Documentation\index.html - html files, June 26, 2008
RCR	GuardianEdge Data Protection Framework 9.0.0 with GuardianEdge Hard Disk Encryption 9.0.0 and GuardianEdge Removable Storage Encryption 3.0.0 Representation Correspondence Version 1.2, April 2, 2008
FRP	GuardianEdge Flaw Remediation Procedure, V1.3, June 23, 2008
ALC	GE Software Development Life Cycle Model V5.4, September 19, 2007
TCD	SFR_Test_Coverage_Analysis(2008-04-22).xls, Test_Coverage_Analysis-20060627-GE_ Response.xls and FuncSpec_Matrix_TestCases.xls "FR/HD b.197.00.02.1, RS b.78.00.02.1"
TP	EAL4 Test Plan for GEFR/GEHD/GERS Version 1.8, April 14, 2008
AT	EAL4_Test_Docs_Tree_Cycle_3(2008-04-30).zip (EAL4_Test_Docs_Tree_Cycle_3 folder)
MA	GuardianEdge Data Protection Framework 9.0.1, GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1 Misuse Analysis, V1.0, May 8, 2008
SOF	Strength of Function Equation 2008-04-22.xls, April 22, 2008
VA	PS 269 – GEHD and GERS Vulnerability Analysis Version 1.5, April 10, 2008
ACM	GuardianEdge Configuration Management (CM) Plan, version 5.1, May 21, 2008
	CI_list.txt, August 22, 2008
	Build Procedures for GuardianEdge Hard Disk Version 1.8, May 23, 2008
	Build Procedures for GuardianEdge Hard Disk Drivers Version 0.2, May 23, 2008
	Build Procedures for GuardianEdge Removable Storage Version 1.6, May 20, 2008
	How to build PBS, V3.1, June 2, 2008
ADO	GuardianEdge Release Procedures, V2.4, January 17, 2008
	SW_download_instructions.htm, September 5, 2007
	GuardianEdge Hard Disk (GEHD) Installation Guide Version 9.0
	GuardianEdge Removable Storage Installation Guide Version 3.0
AGD	**GuardianEdge Hard Disk (GEHD) Encryption Client Administrator Guide version V9.0**

Acronym	Document Title
	GuardianEdge Removable Storage Encryption Policy Administrator Guide V3.0
	GuardianEdge Removable Storage Encryption Client Administrator Guide V3.0
	GuardianEdge Removable Storage Encryption User Guide V3.0
	GuardianEdge Hard Disk Encryption User Guide V9.0
	GuardianEdge Common Criteria Supplement V1.2, August 18, 2008
ISP	GuardianEdge Information Security Policy Version 20060911
DSQ_1	Development Security Questionnaire: Outworx Corp. Date2007_09_07
DSQ_2	Development Security Questionnaire: ZEN Electronics Ltd Date 2007_11_15

6.1 IT Product Testing

At EAL 4 augmented with ALC_FLR.3, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests." (ATE_IND.2, 14.9.5.1 [CEM])

At EAL 4 augmented with ALC_FLR.3, the developer's test evidence must "demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification." (ATE_COV.2, 14.9.2.3)

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

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

The developer and evaluator independent/penetration testing was conducted at GuardianEdge, 475 Brannan Street, Suite 400, San Francisco CA 94107-5421

The Independent testing was performed over a week period from 8/11/08–8/18/08. Installation Testing was performed the first day. Developer testing was performed from 8/4/08–8/8/08, three days in prior to Evaluator Testing. The test plan and results, as well as the evaluation team's review of the testing in the Evaluation Technical Report, were well written and complete.

6.2 Developer Testing

The test approach consists of manual tests that were grouped together under the TOE component being tested. The tests were designed to cover all of the security functions as described in the SFR and TSS section of the ST.

The test plan and procedures do not cover every possible combination of parameters for a given interface and every possible combination of parameters for a given security function. However, the test plan and procedures do stimulate every external interface and all of the security functions.

The individual tests were performed and the results were collected and verified by the developer. The results were archived, recorded, and sent to the evaluator for review.

The vendor's testing purposefully intended to cover all the security functions of Security Audit, Cryptographic Support, Data Protection, Identification and Authentication, Security Management, TOE Protection, and Access Banner, as defined in Section 6 of the ST.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL4 evaluation.

6.3 Evaluator Independent Testing

The test approach consists of providing full coverage of all the TOE's security functions between the developer tests and team-defined functional tests as required under EAL 4.

6.3.1 TEST HARDWARE

GuardianEdge provided the test setup for CygnaCom testing. The figure below shows logical connections. The test setup was intended to be consistent with the available GuardianEdge test facilities.

- **Client Computers**: Windows XP Service Pack 3, Intel platform, hard disk and removable storage components and device drivers
- **Manager Computer**: Windows 2003 Server, Intel platform with storage media for the client installation package files.
- **Generic removable storage devices and CD/DVD devices**: (Dell Latitude D610, 512 MB RAM, CPU 1.6 GHz, HDD speed 4200 rpm, OCZ technology - Rally 4GB flash drive)

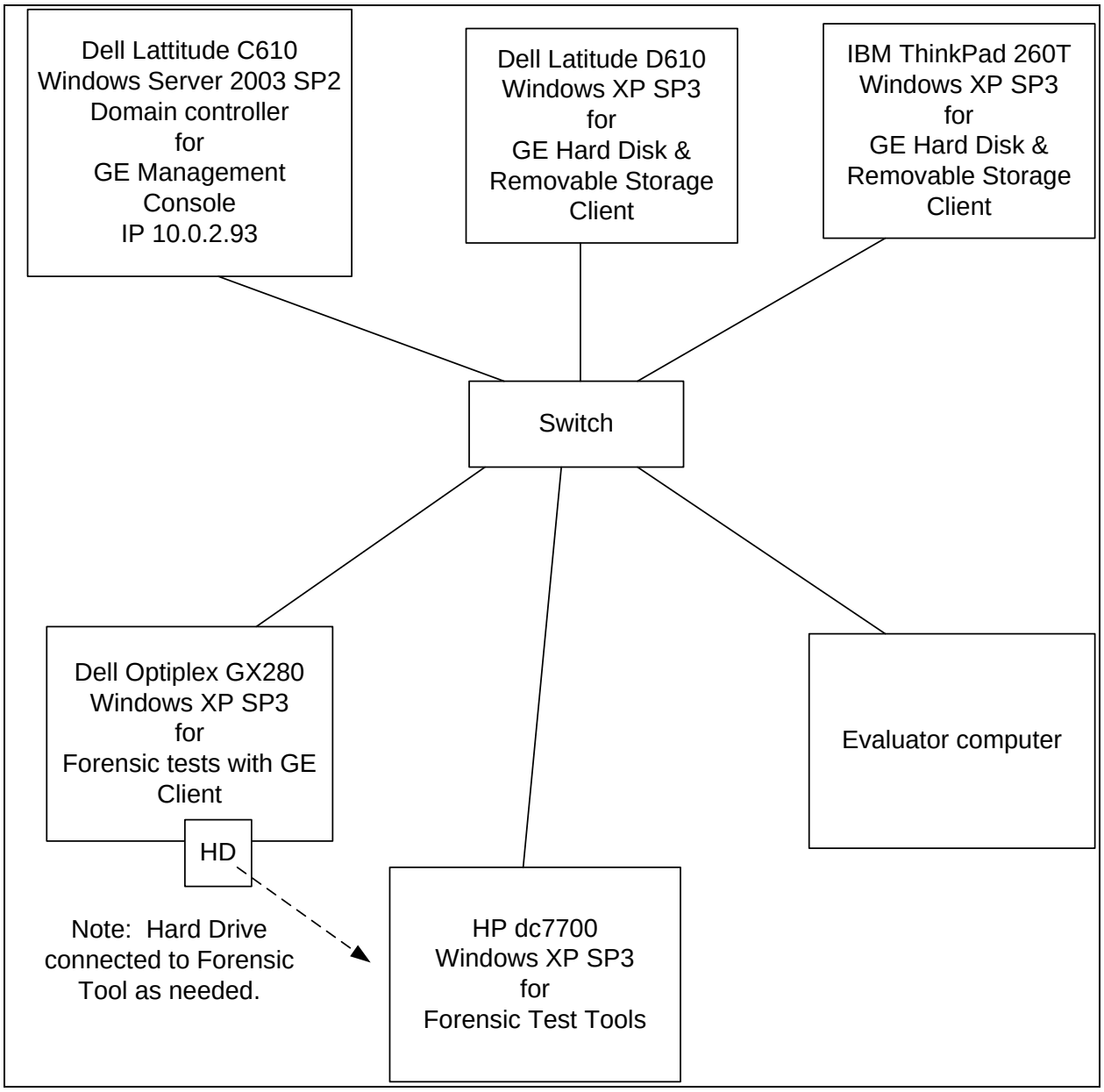

Figure 2. Test Hardware

6.3.2 TEST SOFTWARE

The following software testing tools were used for testing the TOE:

- Event Viewer—system application
- AccessData FTK Imager Version 2.2
- AccessData FTK Version 1.60
- Encase Enterprise Version 6.7.1.3

- Sysinternals Process Explorer 11.4
- Acronis DiskEditor 6.0

All tools were available at Guardian Edge facility and were used for Developer tests.

6.4 Strategy for Devising Test Subset (Developer and Team Defined Tests)

CygnaCom selected 26 of 28 (92%) tests that GuardianEdge provided as evaluation evidence. The tests were selected to exercise security functions from the externally visible TSFI.

The evaluation team ensured that the test sample was sufficient to ensure that:

- All Security Functions were tested
- All External interfaces were exercised
- All Security Functional Requirements were tested

As the product is a Disk/Storage Encryption Decryption product, the emphasis of testing was on both the Identification and Authentication functionality (I & A) and Information Flow Control (FDP_IFC/IFF on-the-fly encryption decryption). The test provided by the developer and the test sample of the developer tests selected tested security functions at appropriate level of rigor.

For cryptographic algorithms claimed in the ST based on both FIPS 140-x standard and by vendor affirmation, the tests did not include testing the correctness of the crypto algorithm or standard. However, testing ensured that a cipher text is created when encrypted and vice versa.

In particular, the SHA-1 algorithm (certificated, but vendor-affirmed) and the Elliptic Curve Cryptography algorithms (vendor asserted) was not analyzed or tested as conforming to cryptographic standards during this evaluation. Those algorithms have only been asserted as tested by the vendor. Other cryptographic algorithms are covered by FIPS certificates.

6.5 Coverage Provided by Devised Test Subset

The evaluator ensured that the test sample sufficient tests such that:

- All Security Functions were tested
- All External interfaces were exercised
- All Security Functional Requirements were tested.

The environment and configuration for the Team-Defined testing has been previously described. A distributed environment was selected to be able to test all of the functionality as described in the ST including optional features. This product can be installed in a number of configurations, including all on one machine.

The independent testing purposefully (directly) covered all of the security functions of, Cryptographic Support, Identification and Authentication, Access Banner, Data Protection, Security Management, TOE Protection, Security Audit, as defined in Section 6 of the ST.

Two tests failed, but these did not indicate failure of covered TOE security functions. Testing resulted in updates to the CC Supplement to the User Guidance, and download Instructions. No obvious vulnerabilities were found.

The following updates were made to the CC User's Guide:

- A CC Supplement to the TOE User Guidance is included as part of the TOE's user guidance.
- Text added to the CC Supplement Appendix D providing a caution about running the chkdsk utility at boot-time, indicating that using chkdsk at boottime could cause the Client Computer to fail to boot.

The following updates were made to the Installation supplements:

- Installation and configuration instructions specific to the evaluated configuration has been published and is included with the TOE's user guidance.

6.6 Strength of Function

The overall strength of function requirement is SOF-medium. The strength of function requirement applies to FIA_SOS.1 which constrains the passwords used for the password-based authentication mechanism defined in FIA_UAU.2 and FIA_UAU.2. The SOF claim for this requirement is SOF-medium. The strength of the "secrets" mechanism is consistent with the objectives of authenticating users (O.PARTIAL_TOE_ACCESS). Strength of Function shall be demonstrated for the password-based authentication mechanisms to be SOF-medium, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a moderate attack potential.

7.0 Evaluated Configuration

The Evaluated Configuration (consistent with the ST):

- *Client Computer*—Windows XP Service Pack 3, Intel platform, hard disk and removable storage components and device drivers
- *Manager Computer*—Windows 2003 Server SP2, Intel platform with storage media for the client installation package files.

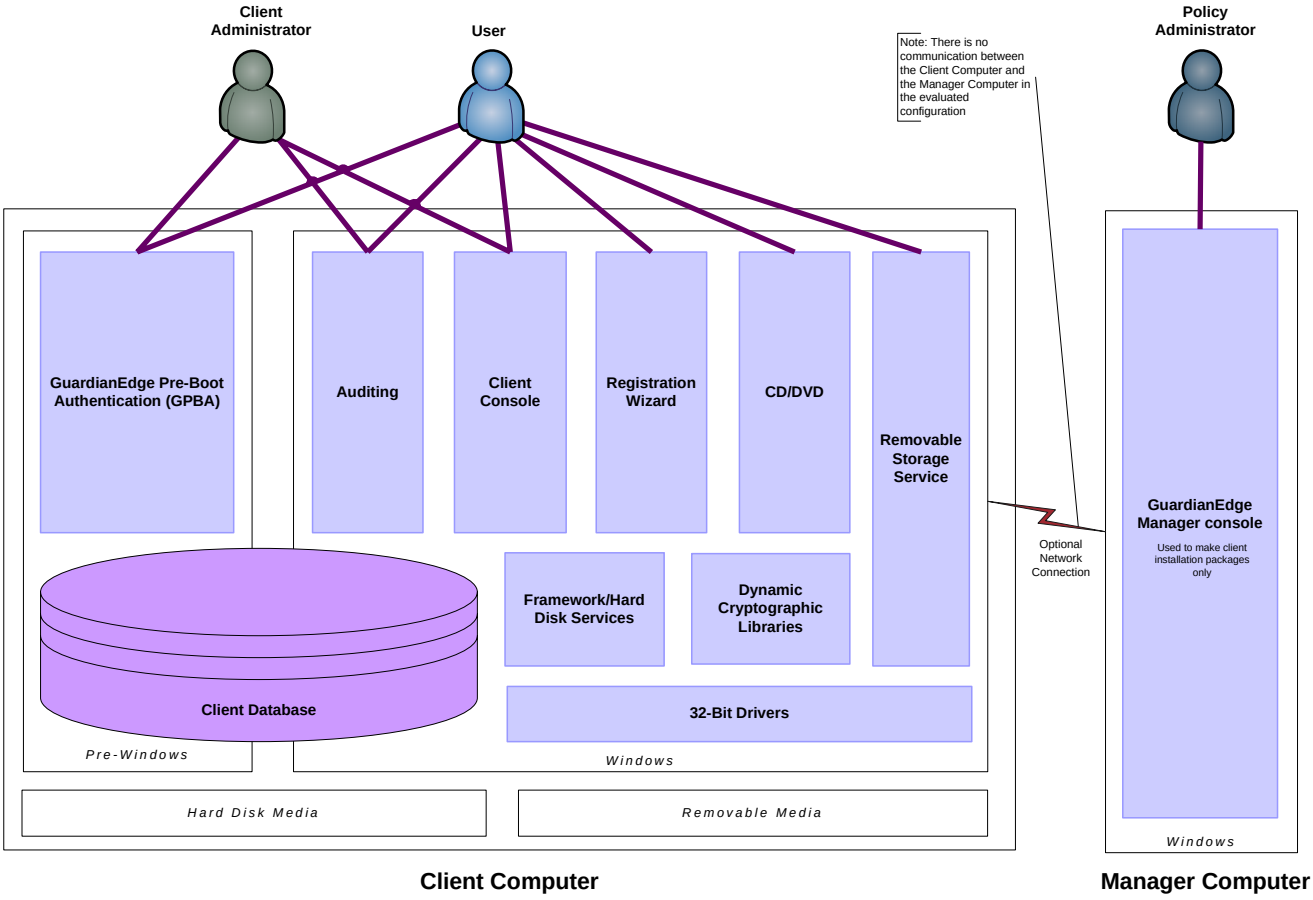

Figure 3. Evaluated Configuration

8.0 Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

- Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 4. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted. ACM_AUT.1 Partial CM Automation
- ACM_CAP.4 Generation Support and Acceptance Procedures
- ACM_SCP.2 Problem Tracking CM Coverage
- ADO_DEL.2 Detection of Modification
- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.2 Fully defined external interfaces
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ADV_SPM.1 Informal TOE security policy model
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance
- ALC_DVS.1 Identification of Security Measures
- ALC_LCD.1 Developer defined life-cycle model
- ALC_TAT.1 Well defined development tools
- ATE_COV.2 Analysis of coverage
- ATE_DPT.1 Testing: high-level design
- ATE_FUN.1 Functional testing

- ATE_IND.2 Independent testing—sample
- AVA_MSU.2 Validation of Analysis
- AVA_SOF.1 Strength of TOE security function evaluation
- AVA_VLA.2 Independent vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant for EAL4 augmented with ALC_FLR.3.
- Strength of Function Rating of SOF-medium

The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9.0 Validator Comments/Recommendations

9.1 User Guidance Version Numbers

The User Guides indicate two-level version numbers, such as 9.0 and 3.0 while the actual TOE contains three-level version numbers, such as 9.0.1 and 3.0.1.

There are no significant differences between 9.0.0 and 9.0.1, or 3.0.0 and 3.0.1, modulo defect repairs. The only updates to provided documentation are increments of the version number on the cover pages.

9.2 Product Functionality Excluded from the TOE

The following product functions are excluded from the TOE:

- Token Authentication (Advanced Authentication)
- Single Sign-On
- Authenti-Check
- One-Time Password

See comments on Lost Password below:

9.3 Lost Password

Although the product supports several methods to recover from a lost or forgotten password, these recovery mechanisms are not part of the TOE. The TOE supports recovery by a Client Administrator. If both the client administrator and the user passwords are lost, the encrypted disk cannot be recovered.

9.4 Power Loss During Initial Encryption

Unexpected power loss during initial encryption process was tested and found that the TOE encryption process was able to safely recover without corrupting data. The encryption process continued to completion when power was restored.

9.5 Removable Media Tested

The following removable storage devices were tested:

- USB Flash Drive
- CD
- DVD
- 1.5 inch floppy disk

- SD card

Note: Although iPods and MP3 players may also be used as removable storage devices, such devices are not supported by the TOE, and encryption of files written to such devices is likely to impact their functionality in the TOE configuration.

9.6 Sharing Encrypted Data with Other Computers

GuardianEdge provides an optional utility that allows for decryption on Windows computers that **do not** have GuardianEdge Removable Storage Encryption installed. However, this utility **is not** part of the current evaluation. GuardianEdge plans to include this utility in a maintenance evaluation at a later date. Without the utility, it is **not possible** to share encrypted data with computers that do not have GuardianEdge Removable Storage Encryption installed.

9.7 Running Defraggers

Running the chkdsk utility at boot-time can damage the Master Boot Record. If used, chkdsk at boot time could cause the Client Computer to fail to boot. See Appendix D of the CC supplement to the user's guide.

9.8 Default Passwords

Use of a Default Password introduces the risk that a breach of the password for one file or device will breach multiple files and devices. On the other hand, users greatly resist having to enter a password for every file written to removable storage. This increases overall security risk since users may attempt to bypass encryption all together.

9.9 Double Encryption

Encrypting data once with a product from one vendor and a second time with a product from another vendor, may prevent future decryption. Some removable storage devices offer encryption services of their own. If the administrator configures the installation of GuardianEdge Removable Storage to always encrypt, users should not utilize any additional encryption services that may be offered, as they may preclude decyrption.

9.10 Recovery from Hard Disk Problems

Recovery from hard disk problems with the recovery utilities is not covered in the ST as it was not tested. GuardianEdge Hard Disk Encryption Client Administrator Guide, Version 9.0 describes the hard disk recovery methods for the product.

9.11 Overflow of the Pre-Boot Authentication (PBA) Buffers

The PBA audit log is on a circular buffer that can store approx 100,000 records therefore it is unlikely recent events could be lost through overflow of the buffer.

9.12 Encryption Library

The TOE uses the GuardianEdge Encryption Plus Cryptographic Library version 1.04.

9.13 Encryption Certificate

The encryption certificates for the product, certificate #515, only applies, with respect to XP, to SP2 (as SP3 wasn't out yet).

Additionally, the certificate indicates "Single-User Mode." The evaluation team concluded that the in this context, the term "Single-User Mode" refers to only one user using the TOE as opposed to booting to a single super user. The validation team concurs that the evaluation is in sync with the FIPS certificate.

9.14 Unevaluated Algorithms

The SHA-1 algorithm (certificated, but vendor-affirmed) and the Elliptic Curve Cryptography algorithms (vendor asserted) were not analyzed or tested as conforming to cryptographic standards during this evaluation. Those algorithms have only been asserted as tested by the vendor. Other cryptographic algorithms are covered by FIPS certificates.

10.0 Security Target

GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1The ST is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of the CC.

11.0 Glossary

The following table is a glossary of terms used within this validation report and evaluation.

CC	Common Criteria
EAL	Evaluation Assurance Level
GEFR	GuardianEdge Framework
GEFS	GuardianEdge File System
GEHD	GuardianEdge Hard Disk Encryption
GMBR	GuardianEdge Master Boot Record
GPBA	GuardianEdge Pre-Boot Authentication
GERS	GuardianEdge Removable Storage Encryption
IT	Information Technology
MBR	Master Boot Record
OSP	Organizational Security Policy
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy
WEK	Workstation Encryption Key

This section defines the Common Criteria terms. Not all of these terms are used in this document.

Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.
Authentication data	Information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.

Bulk Encryption The encryption of large amounts of data. This is as opposed to key encryption.

Class A grouping of families that share a common focus.

Component The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Connectivity The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Element An indivisible security requirement.

Evaluation Assessment of a PP, an ST, or a TOE against defined criteria.

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.

Evaluation scheme The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Human user Any person who interacts with the TOE.

Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.
Initial Encryption	The encryption of the designated hard disk partitions that follows the installation of GuardianEdge Hard Disk Encryption is called initial encryption. This is as opposed to terminal decryption.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Iteration	The use of a component more than once with varying operations.
Key Encryption	Encryption of keys for key management purposes. This is as opposed to bulk encryption.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Organizational security policies	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.
Package	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Reference monitor	The concept of an abstract machine that enforces TOE access control policies.
Reference validation mechanism	An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Security attribute	Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.
Security Officer	Person responsible for setting IT security policies at an organization.
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by threat agents possessing a low attack potential.
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by threat agents possessing a moderate attack potential.
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized

	breach of TOE security by threat agents possessing a high attack potential.
Subject	An entity within the TSC that causes operations to be performed.
System	A specific IT installation, with a particular purpose and operational environment.
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Terminal Decryption	Terminal decryption refers to the decryption of encrypted hard disk partitions. In the TOE, only the Client Administrator can perform this task. This is as opposed to initial encryption.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface (TSFI).	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.
Transfers outside TSF control	Communicating data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence to support the TSP.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data	Data created by and for the user that does not affect the operation of the TSF.

12.0 Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- GuardianEdge Technologies (http://www.guardianedge.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.

Other Documents

- [ST] GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1