National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Encryption Plus® Hard Disk 7.0

Report Number: CCEVS-VR-03-0037
Dated: 9 April 2003
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Kathy Cunningham
Margaret Webster-Butler
National Security Agency
Ft. Meade, MD 20755

Common Criteria Testing Laboratory

Evaluation Team
CygnaCom Solutions, an Entrust Company
7927 Jones Branch Drive
McLean, VA 22102

Table of Contents

1 Executive Summary

The evaluation of the PC Guardian Encryption Plus® Hard Disk 7.0 was performed by CygnaCom Solutions CCTL in the United States and was completed on 26 March 2003. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Encryption Plus® Hard Disk 7.0 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The CygnaCom Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL1) have been met.

The technical information included in this report was obtained from the Security Target (ST) produced by PC Guardian and the Evaluation Technical Report (ETR) (non-proprietary) produced by CygnaCom Solutions.

1.1 Evaluation Details

Dates of Evaluation: August 2002 through March 2003
Evaluated Product: Encryption Plus® Hard Disk 7.0
Developer: PC Guardian
CCTL: CygnaCom Solutions, McLean, VA
Validation Team: Kathy Cunningham, National Security Agency, Ft. Meade, MD
Evaluation Class: EAL1
PP Conformance: None

1.2 Interpretations

National Interpretations

I-0347 Including Sensitive Information In Audit Records
I-0375 Elements Requiring Authentication Mechanism
I-0389 Recovery To A Known State
I-0393 A Completely Evaluated ST Is Not Required When TOE Evaluation Starts
I-0395 Security Attributes Include Attributes Of Information And Resources
I-0459 CM Systems May Have Varying Degrees Of Rigor And Function
I-0405 American English Is An Acceptable Refinement
I-0406 Automated Or Manual Recovery Is Acceptable
I-0407 Empty Selections Or Assignments
I-0409 Other Properties In FMT_MSA.3 Should Be Specified By Assignment
I-0411 Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR
I-0416 Association Of Access Control Attributes With Subjects And Objects
I-0418 Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
I-0420 Attribute Inheritance/Modification Rules Need To Be Included In Policy
I-0425 Settable Failure Limits Are Permitted
I-0426 Content Of PP Claims Rationale
I-0427 Identification Of Standards
I-0429 Selecting One Or More

International Interpretations

008 Augmented and Conformant overlap
009 Definition of "Counter"
019 Assurance Iterations
027 Events and functions in AGD_ADM
032 Strength of Function Analysis in ASE_TSS
038 Use of 'as a minimum' in C&P elements
043 Meaning of “clearly stated” in APE/ASE_OBJ.1
049 Threats met by environment
051 Use of 'documentation' without C&P elements
055 Incorrect Component referenced in Part 2 Annexes, FPT_RCV
058 Confusion over refinement
064 Apparent higher standard for explicitly stated requirements
065 No component to call out security function management
067 Application notes missing in ST
069 Informal Security Policy Model
084 Separate objectives for TOE and environment
085 SOF Claims additional to the overall claim
098 Limitation of refinement
120 Sampling of process expectations unclear
127 TSS Work unit not at the right place

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.PAS_LOS: The user may forget their password, making data unavailable. There is no third party threat agent with this threat; rather a memory lapse on the part of an authorized user presents the threat that the user will lose access to their data.

T.DSK_COR: The disk may become corrupted due to mechanical failure or unclean operating system shutdown due to power interruption. There is no third party threat agent with this threat, though the mechanical failure could potentially be intentionally induced by a threat agent with the intent of denying the user access to his data.

T.DAT_SEC: A threat agent who has exploited an opportunity to gain physical access to the machine may try to examine data stored on disk to find user data that is stored in protected partitions.

T.USR_LOG: A threat agent who has exploited an opportunity to gain physical access to the machine may try to abuse the User Program logon mechanism to gain access to the user's data.

T.UAD_LOG: A threat agent who has exploited an opportunity to gain physical access to the machine the User Program is installed on may try to execute the User Program Admin Logon protocol in an attempt to gain access to the user's data.

T.ADM_LOG: A threat agent who has exploited an opportunity to gain physical access to the machine the Administrator Program is installed on may try to abuse the Administrator Program logon mechanism to gain access to the functions of the Administrator Program.

T.REC_USR: The threat agent may be another EP Hard Disk user who has stolen or otherwise gained physical access to the target user's machine. The threat agent may try to execute the access recovery procedure authenticating as himself in an attempt to gain access to the target user's data.

T.REC_EAV: The threat agent may eavesdrop on the telephone or other communications between the user and the administrator to capture the messages exchanged during the access recovery procedure. The threat agent will then after the fact attempt to steal or otherwise gain detectable access to the computer and try to use the recovery information eavesdropped to gain access to the user's data by using it to execute the recovery procedure.

T.ATK_LOG: A threat agent who has exploited an opportunity to gain physical access to the machine may try to gain access to the machine via the Authenti-Check logon function with the aim of gaining unauthorized access to user data.

T.UPD_MOD:The threat agent may try to modify configuration and password updates the User Program receives from the administrators. If the threat agent could modify the administrator password update, it could replace the administrator's new EC public key in the update message and hence be able itself to execute the User Program Admin Logon protocol on the user machine if he could gain physical access. Configuration option updates are also of relevance to security, in that if the threat agent could modify contact information in the application he may be able to

more easily socially engineer passwords or other sensitive information from the users, who may then incorrectly assume the threat agent is a trusted company administrator. The aim of these attacks is to gain unauthorized access to user data.

T.ADM_CFG: The administrator may unintentionally select insecure configuration parameters or insecure default configuration parameters for the user. The risk if insecure configuration parameters are selected is that a threat agent could attempt to gain access to user data with fewer restrictions than intended by the administrator.

T.USR_CFG: The user may unintentionally select insecure configuration parameters, reducing the security of the TOE. The user may try to select values that the EP Hard Disk Administrator considers inappropriate for the environment the installation is used in. The risk if insecure configuration parameters are selected is that a threat agent could attempt to gain access to user data with fewer restrictions than intended by the user.

T.SW_BUG: The TOE may exhibit a software bug and fail to protect the user data.

T.DAT_LEK: If the user configures the software to have some encrypted and some unencrypted partitions the user may accidentally write data intended to be protected to an unprotected partition. Application software may write user data to unprotected partitions without the user's knowledge.

T.DB_SEC: If the Administrator Database contents were obtained by a threat agent, the threat agent could execute the User Program Admin Logon protocol on any installation of the User Program in the Corporate Administrator's domain of control and thereby gain unauthorized access to user data.

T.BAK_DBK: If the Administrator Database key were obtained by a threat agent who was also able to copy the Administrator Database, the threat agent could execute the User Program Admin Logon protocol on any installation of the User Program in the Corporate Administrator's domain of control, thereby gaining unauthorized access to user data. If the Administrator Database key were lost and the corresponding passwords forgotten, the Administrator Program functions would become unavailable. In this event availability of user data could be lost if the user forgets their password as the recovery function and admin logon would no longer be available.

2. Identification

2.1 ST and TOE Identification

ST: PC Guardian Encryption Plus® Hard Disk 7.0 (EAL1), Version 1.02, March 24, 2003.

TOE Identification: Encryption Plus® Hard Disk 7.0 Software Application.

This is a software only TOE. The complete software application was evaluated. The hardware and operating system used in the evaluation are outside the scope of the evaluation.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

The Encryption Plus® Hard Disk 7.0 software package (hereinafter referred to as EP Hard Disk) is a hard disk encryption system that encrypts entire disks or partitions at the disk driver level so that normal applications can use the EP Hard Disk confidentiality services transparently. EP Hard Disk includes features for site installation, administration, and recovery from lost passwords.

EP Hard Disk is a hard disk encryption system that encrypts entire disks or partitions at the disk driver level so that normal applications can use the EP Hard Disk confidentiality services transparently. EP Hard Disk 7.0 software package is available for Windows 2000, XP, and NT versions of the Microsoft Windows family of operating systems, which were outside the scope of the evaluation.

The data written to and read from the partition or disk are respectively encrypted and decrypted on-the-fly as required, driven by operating system use of the storage device.

2.2 IT Security Environment

The TOE environment runs only trusted software that has been approved by the security officer. If the computer is connected to a network, either file sharing and other network services offering remote access to data stored on the computer are disabled, or appropriate authentication and confidentiality services are used in combination with those services and authenticated remote users are considered to be within the domain of authorized users.

3. Security Policy

There are no Operational Security Policies defined for the TOE.

4. Assumptions

4.1 Personnel Assumptions

A.TRU_ADM: Personnel fulfilling administrative roles in the TOE's operation are trustworthy. If EP Hard Disk administrators have privileges allowing them to gain access to user data, it is

assumed that they are trustworthy and do not attempt to make unauthorized disclosures of confidential data or disclose administrator passwords allowing recovery of confidential data.

A.USR_ATH: When the administrator assists the user in recovering access to their data with the One-Time Password Program, the administrator must assure himself or herself of the user's identity. This is to prevent a threat agent — who has stolen or gained unattended access to the user's machine while it is not logged on — from using the access recovery procedure by pretending to be the user. The administrator is assumed to use some reliable and secure method to authenticate users.

4.2 Physical Assumptions

A.PHY_CTL: The computer the User Program is installed on should not fall under temporary and undetected physical control of a threat agent. Appropriate physical security measures and physical security policies are in place to manage risk of this event occurring.

A.REC_PHY: The computer the One-Time Password Program is installed on should not fall under the physical control of a threat agent.

A.PWR_LOS: When the option to disable power-loss recovery during initial encryption is used it is assumed that no user data (or no non-backed up user data) is on the disk, and that the machine is connected to a reliable source of power with sufficient capacity to complete the operation.

5. Architectural Information

All underlying hardware on which the TOE operates is not considered to be part of the TOE.

The TOE is not a networked system and executes locally, therefore, a networking interface is not included as a physical TOE or non-TOE component.

Hardware components not considered part of the TOE, yet at a minimum, are required for TOE operation, are the following:

- Windows NT/2000/XP Operating Systems
- 800x600 video resolution or higher
- 16-bit color resolution or higher
- BIOS support extended INT 13
- Up to 1 Terabyte with up to 8 logical partitions

6. Documentation

Purchasers of the PC Guardian Encryption Plus® Hard Disk will receive Administrator Guide and User Guide documentation Enterprise-Version 7.0 revised 12/13/02.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1 Developer Testing

As this was an EAL 1 evaluation, developer testing was not supplied as part of the documentation.

7.2 Evaluation Team Independent Testing

The Evaluation Team developed independent test sets that covered a range of conditions to verify functions defined by the administrative or user guidance. As these scenarios were conducted, the actual tests performed by team members were documented in more detail along with the expected and actual test results. Any associated procedures have also been detailed and documented. A total of 45 different test configurations were tested. Complete test configuration and procedures are contained within section 3.1.7 Testing Assessment of the PC Guardian Encryption Plus® Hard Disk, Evaluation Technical Report, dated 26 March 2003.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures resulted in a secure configuration.

8. Evaluated Configuration

The evaluated configuration consisted of Encryption Plus® Hard Disk 7.0 running Administrator and User Programs on a Dell Latitude CPx, Pentium II 266 MHz Processor 128 MB RAM 4 GB Hard Drive running Windows XP and a User Program on IBM Desktop Intel Celeron processor 668 Mhz with 256 MB of RAM running Windows XP.

9. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL1 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 3, Evaluation Results in the Evaluation Team's ETR states:

"The verdicts for each CEM work unit in the ETR sections are each "PASS". Therefore, when configured according to the provided OEM guidance documentation, the PC Guardian Encryption Plus® Hard Disk 7.0 satisfies the PC Guardian, Encryption Plus® Hard Disk 7.0 Security Target, Version 1.02, March 24, 2003."

Section 4, Conclusions in the Evaluation Team's ETR states:

"The evaluation satisfied the assurance requirements for EAL1."

10. Validation Comments/Recommendations

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11. Abbreviations

Abbreviations	Long Form
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CM	Configuration Management
EAL	Evaluation Assurance Level
EPHD	Encryption Plus® Hard Disk 7.0

Abbreviations	Long Form
ETR	Evaluation Technical Report
FSP	Functional Specification
ID	Identification
IT	Information Technology
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
PC	Personal Computer
PP	Protection Profile
QA	Quality Assurance
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSS	TOE Summary Specification

12. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.