National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Check Point Endpoint Security Full Disk Encryption, Pointsec PC 6.3.1

Report Number:	CCEVS-VR-VID10194-2009
Dated:	1 August 2009
Version:	2.0

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

Scott Shorter, Lead Validator

Deborah D Downs, Senior Validator

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 10 June 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Metatron Security Services. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and meets the assurance requirements of EAL4 augmented with ALC_FLR.1. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1. The TOE, is a hard disk encryption application that contains an embedded cryptographic module that is certified against FIPS 140-2 Level 1 (certificate#770), which is used for all cryptographic functions. The product is a software based security product for the Windows based PC platform that employs both boot authentication and transparent disk encryption to provide complete protection of information resources stored on fixed media in a desktop, workstation, or laptop.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

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 and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's 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 Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Pointsec PC 6.3.1
Protection Profile	Not applicable
ST	Check Point Endpoint Security Full Disk Encryption Security Target, Version 2.4, 22 June 2009
Evaluation Technical Report	Evaluation Technical Report For Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1 (Non-Proprietary), Version 1.0, 2 July 2009, Part 2 (Proprietary), Version 2.0, 2 July 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Item	Identifier
Conformance Result	CC Part 2 conformant and Part 3 conformant, EAL4 augmented with ALC_FLR.1
Sponsor	Check Point Software Technologies Inc.
Developer	Check Point Software Technologies Inc.
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Terrie Diaz, Dawn Campbell, Quang Trinh
Validation Body	NIAP CCEVS: Scott Shorter, Lead Validator Deborah Downs, Senior Validator

3 Organizational Security Policy

This section summarizes the security functions provided by Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1 that is evident at the various identified network interfaces. It is based on information provided in the Security Target.

3.1 Security audit

The TOE collects audit data and provides an interface for authorized administrators to review audit logs. Audit information generated by the system includes date and time of the event, user ID that caused the event to be generated, computer where the event occurred, and other event specific data. The TOE also restricts log access to authorized users.

3.2 Cryptographic support

The TOE’s Cryptographic Support security function implements several security functions. The cryptographic support mechanisms can be categorized as cryptographic key management and cryptographic operations. The cryptographic functionality of the TOE is based upon the FIPS 140-2 validated Pointsec Cryptographic Module (FIPS 140-2 certificate #770) embedded in the product. The certificate numbers for the FIPS approved algorithms are HMAC FIPS198 certificate#202, AES FIPS197 certificate#430 and Triple DES FIPS46-3 certificate#459.

3.3 Identification and authentication

The TOE supports multiple user authentication mechanisms enabling the administrator to assign appropriate authentication requirements for the intended environment, including:

- Fixed password (username/password),

- Smart card (and USB token with embedded smart card) based authentication (smart card/PIN).
- Remote Help authentication (username/phone identification/TOE challenge/Admin response). Remote Help is divided into two types, one-time login and remote password change. These provide a way to authorize a user to login when the normal authentication process can not be performed, such as when the user forgets their smart card at home, or a fixed password has been forgotten.

Where a smart card is used for authentication, the card and reader (or token) are part of the IT environment.

User authentication is done in the pre-boot environment and the operating system will not boot up unless an authorized user is authenticated. In addition, administrators authenticate using the same mechanisms as above prior to gaining access to the Pointsec for PC Management Console application.

3.4 Security management

The TOE administration is designed to enable central control of policy and security settings, decentralized deployment and day-to-day administration. Pointsec for PC should be administered using several different levels of authority. It can be administered from the Pointsec for PC Management Console (PCMC) on any computer that has the product installed on it. This gives the administrators control and easy access to higher-level functionality without being tied to one computer.

3.5 Protection of the TSF

Pointsec for PC implements a specific set of security mechanisms to ensure that security functions cannot be bypassed or tampered with. To prevent bypassing of the TOE security functions, the TOE takes control of the Boot Sector of the boot partition, which prevents access to the system without successful authentication. The Boot-code is checked for the presence of debugging tools at each step of the loading process. If suspicious code is detected, the boot process will stop. Within the Windows operating system, Pointsec for PC functions as a kernel mode process, restricting access to its execution space and memory. When the TOE starts (from Power on) it has its own OS and is later handing over control to Windows after it has authenticated the user and recreated the encryption key. During that time, Pointsec is in control Windows security does not matter.

3.6 Fault Tolerance

When a Pointsec PC workstation/laptop loses contact with the file share server, the TOE provides the administrator with the capability to identify additional three servers for redundancy. As a result, if a server is offline, or the workstation/laptop is unable to contact it, the workstation/laptop will attempt to communicate with one of the other identified servers. Even if no storage resource is accessible the TOE will continue to operate as normal.

3.7 Trusted path

For initial logon, a user must invoke a trusted path in order to ensure the protection of identification and authentication information. The trusted path is invoked by a system reset which is always captured by the TOE (i.e. it cannot be intercepted by an untrusted process).

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed those responsible to manage the TOE are competent individuals that only authorized users can gain access to the TOE, and will follow and abide by the instructions provided by the TOE documentation.
- It is assumed Authorized users of the TOE will keep all their authentication data private.
- The IT environment will provide a storage resource for the management of the TOE installation files, recovery files, update profiles, and software updates.
- The IT environment will provide a reliable time source to enable the TOE to timestamp audit records.
- The system personnel maintain a TOE-independent database containing a list of authorized TOE users and administrators along with unique, non-TOE authentication data that can be used to verify identity over a phone connection (i.e. no video, only voice communications) for the purposes of providing Remote Help authentication to authorized TOE users.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- Users of the system shall be held accountable for their security relevant actions within the system.
- The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE.
- All cryptographic operation performed by the system will be compliant with the requirements of FIPS 140-2 Level 1.
- The system must have the ability to protect system data in transmission between distributed parts of the protected system.
- The system must ensure that security functions continue to operate if contact with the file share is lost.

The TOE encrypts the entire disk sector by sector including the system files, temp files, deleted files and unused space. The encryption is user transparent and automatic, so there is no need for user intervention or user training. Because the encryption occurs in the background without noticeable performance lost, there is no user downtime.

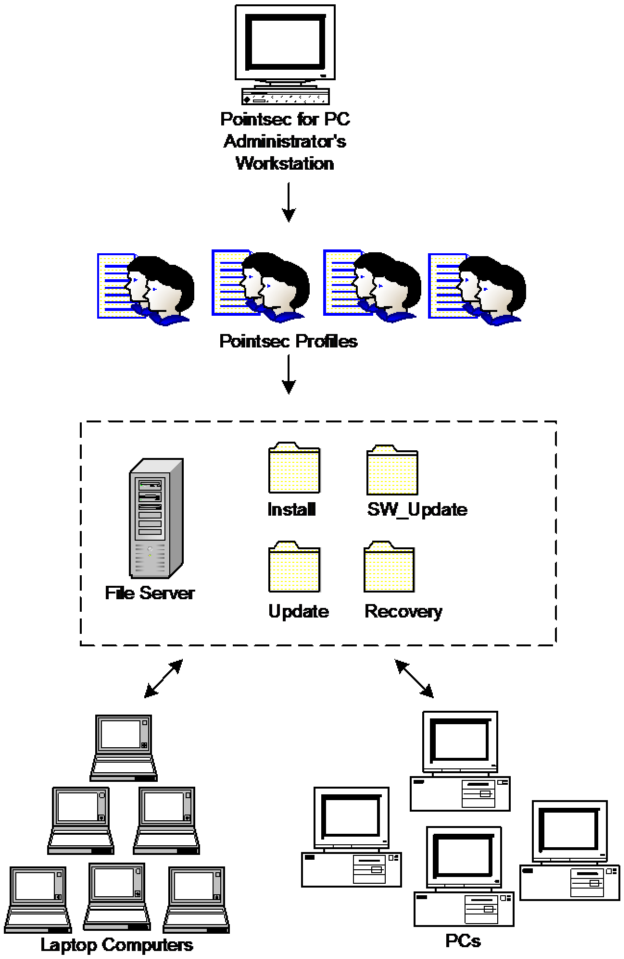
5 Architectural Information[1]

Pointsec PC 6.3.1 is a disk encryption product that can be centrally administered throughout the enterprise. The TOE employs both boot authentication and transparent disk encryption to provide protection of information resources stored on fixed media in a workstation or a laptop. Pointsec PC is a software based security product, for the Windows based PC platform. The product contains an embedded cryptographic module that is certified against FIPS 140-2 Level 1 (certificate#770), used for all cryptographic functions.

Since the TOE is a software product, its physical boundary is defined by the physical case of the computer where it is installed. The TOE can be installed on any x86 compatible computer running Microsoft Windows 2000, Microsoft Windows XP Professional and Windows XP Tablet PC Edition, Microsoft Windows Server 2003 and Microsoft Windows Vista. Microsoft .NET Framework 2.0 or later is required for PCMC.

Installation files, recovery files, update profiles, and software updates can be stored on a storage resource outside of the TOE’s physical boundary (e.g. file server), as shown in figure 2. This provides member workstations/laptops with a central point for storage. All security related files (profiles, central log files, and recovery files) are encrypted before they are stored on the server. Access to the server itself is configured through the server (instructions are detailed in the installation guide and administrator’s guide). The server where the file share resides is not part of the TOE but the IT-environment. No components of the TOE need to be installed on the file server. Separate instances of the TOE are installed on the administrator’s workstation and each of the laptops or PCs included in the system.

[1] Extracted from SAIC Final ETR Part 1 Version 1.0, 2 July 2009



6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

6.1 Design documentation

Document	Version	Date
Pointsec for PC Functional Specification	Version 2.2	17 March 2009
Pointsec for PC High-level Design	Version 2.2	17 March 2009
Pointsec for PC Low-level Design	Version 2.2	17 March 2009
Pointsec PC 6.2 Code Review and Correspondence LLD to IMPL	Version 1.2	10/05/2007
Pointsec for PC Security Policy Model	Version 2.4	17 February 2009

6.2 Guidance documentation

Document	Version	Date
Pointsec PC Administrator's Guide	Version 6.3.1	June 22, 2009
Pointsec PC Installation Guide	Version 6.3.1	March 17, 2009

6.3 Configuration Management and Lifecycle documentation

Document	Version	Date
Pointsec Configuration Management Manual	Version 1.3	09/04/2008
Bug Analysis and Correction Process	Revision 0.92	9 Dec 2007
Change Control Process	Version 1.1	18 April 2007
All Submitted Documents	Version 10	11 July 2007
CD video evidence		
Software Development Process	Revision 1.2	16 February 2007
Sundsvall Network	Version 1.1	11 June 2006
Life Cycle Support – Development Security	Revision 1.3	20 June 2007
Employee Contract / Confidentiality agreement		

6.4 Delivery and Operation documentation

Document	Version	Date
Pointsec Software Product Delivery Manual	Version 1.6	March 30, 2007
Pointsec PC Installation Guide	Version 6.3.1	March 17, 2009

6.5 Test documentation

Document	Version	Date
Check Point Endpoint Security Full Disk Encryption 6.3.1 Test Documentation	Version 0.9.7	June 18, 2009

The actual test results have been submitted to the evaluation team, as screenshots are result files.

6.6 Vulnerability Assessment documentation

Document	Version	Date
Pointsec Vulnerability Analysis	Version 2.0	4/27/2009
Pointsec For PC Strength of Function	Version 2.2	5/11/2008
Pointsec for PC Misuse Analysis	Version 2.2	27 April 2009

6.7 Security Target

Document	Version	Date
Check Point Endpoint Security Full Disk Encryption Security Target	Version 2.4	6/22/2009

7 IT Product Testing

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

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, Cryptographic support, Identification and authentication, Security management, and Protection of the TSF, Fault Tolerance, Trusted Path. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer’s actual test results matched the vendor’s expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire developer’s manual test suite on Windows XP and Windows Server 2003. In addition to re-running the developer’s tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the developer’s test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the TOE software for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
  - Any hardware that supports the TOE components is acceptable. (Note: TOE is software only product)
- IT Environment Hardware
  - Any hardware that supports the non-TOE IT components is acceptable. For example, workstation, laptop, reader, smart card, etc.
- Test Hardware
  - No specific test hardware is required

- Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment.

The following software is required to be installed on the machines used for the test:

- TOE Software
    - Pointsec PC v6.3.1
- IT Environment Software
    - Windows XP Professional, Windows Server 2003, and Windows Vista (Note: Vista platform was not tested because the product does not support 64-bit Windows Vista platform and the lab only has license for 64-bit Vista.)
    - Microsoft .NET Framework 2.0 or later
    - Aladdin PKI drivers for Windows, Version 4.55.22
    - Smart Card: Aladdin eToken 32k
- In addition, the following software is required in support of the test cases:
    - VM-Ware Version 6.0
    - SoftICE debugger tool
    - WireShark v1.0.2
    - WinHex v14.0

7.3 Penetration Testing

The evaluators developed penetration tests to address the Input Validation, Network Sniffing, Analysis of AdminPC and ClientPC communication, and Verify TOE is using the FIPS 140-2 module security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The TOE, Pointsec PC 6.3.1 is installed on a desktop, workstation, or laptop. Pointsec PC 6.3.1 is compatible with the following Microsoft Operating Systems: Windows 2000, Windows XP Professional and Windows XP Tablet PC Edition, Windows Server 2003 and Windows Vista.

There are two installation types in Pointsec PC:

- Master Installation:

The Pointsec PC program is first installed and configured on a Pointsec PC system administrator computer. Once Pointsec PC has been configured on that computer, the system administrator can configure a Pointsec PC installation profile containing all the information and software necessary to install and manage Pointsec PC on the PCs to which it is deployed on the Client.

- Client Installation:

In Common Criteria validated environments, all administration and configuration of client installations must be done via profiles. All updates and new installation profiles for both clients and administration are then maintained via profiles, created on a master installation. In a Common Criteria validated environment, only silent installation profiles should be used to deploy Pointsec PC.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on February 2007. The evaluation confirmed that the – Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 conformant, and assurance requirements (Part 3) for EAL4 Augmented with ALC_FLR.1. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Check Point Endpoint Security Full Disk Encryption Security Target, Version 2.4, dated June 22, 2009.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the Check Point Endpoint Security Full Disk Encryption; Pointsec PC 6.3.1 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition, the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications is properly controlled.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

The evaluation team followed the Pointsec PC Version 6.3.1 Installation Guide and Pointsec PC Version 6.3.1 Administrator's Guide installation (and configuration) procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL4 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The Pointsec PC Version 6.3.1 Installation Guide and Pointsec PC Version 6.3.1 Administrator's Guide were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied the ALC_FLR.1 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high-level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, misuse analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR. The validation team therefore recommends that the evaluation results be accepted.

If communication with the file share for log file transfer is disrupted for a sufficient period of time, it is theoretically possible for records to be overwritten. Testing did not verify this or determine what that period of time would be.

11 Security Target

The Security Target is identified as Check Point Endpoint Security Full Disk Encryption Security Target, Version 2.4, June 22, 2009. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL4 augmented with ALC_FLR.1.

12 List of Acronyms

AES	Advanced Encryption Standard
BIOS	Basic Input/Output System
BS	Boot Sector
CBC	Cipher Block Chaining
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
EW	Enterprise Workplace

FIPS	Federal Information Processing Standards Publication
GAL	Group Authority Level
GB	Gigabyte
I/O	Input/Output
MAC	Message Authentication Code
MBR	Master Boot Record
NIST	National Institute of Standards and Technology
PCMC	Pointsec for PC Management Console
PBE	Pre-Boot Environment
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RSA	Rivest Shamir Adleman (public key algorithm)
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functions
TSP	TOE Security Policy

13 Glossary of Terms

- **Administrator:** Accounts at this level have limited authority in the administration of the TOE (according to what has been defined in the system settings). The Administrator can typically view logs and provide remote help. Administrators can not raise their own authorization level.

- **Authentication data:** Information used to verify the claimed identity of a user.

- **Authorized administrators:** A term used to encompass both the Administrator and System Administrator roles defined in this ST.

- **Authorized users:** A term used to describe all users that interact with the TOE that have a unique identifier. This includes the non-privileged set of users and all others within the Administrator and System Administrator groups.

- **Disk Partition:** A logical division of a hard disk. Each partition can be formatted for a different file system. A partition must be completely contained on one physical disk. The Master Boot Record for a physical disk can contain up to four entries for partitions, including one extended partition, which can be further subdivided into logical volumes, allowing for more than four partitions on one physical disk.

- **File Share:** A storage resource where installation files, profiles, recovery files and software updates can be stored. System Administrators are able to utilize the share to install and configure the system, delegate authorization, modify the system for local conditions, and assign the properties and authorization of individual users by using profiles.

- **FIPS 140-2:** Federal Information Processing Standards Publication published by the National Institute of Standards and Technology (NIST) to define security requirements for cryptographic modules.

- **Fixed password authentication:** A normal password authentication mechanism. The administrator can make changes to the default requirements for passwords.

- **Group Authority Level:** a numeric authorization (0-9) associated with user groups and with system settings, defining a restriction for the objects that each user group may administer.

- **Identity:** A representation uniquely identifying an authorized user.

- **One-time Login authentication:** An authentication mechanism whereby a user who normally authenticates with a smart card is granted temporary, one-time access to the TOE. See Remote Help authentication mechanisms.

- **Partition key (K_P):** A symmetric encryption key that is used by the TOE to encrypt individual partitions on a hard drive.

- **Remote Help authentication mechanism:** A secondary authentication mechanism, only used in special circumstances, where the user requests login assistance from authorized personnel over the phone. This mechanism uses a challenge-response sequence that is read over the phone to provide the user authorization for access to the TOE. There are two types of Remote Help, One-time login and Remote Password Change. These mechanisms provide temporary authentication to the TOE when normal authentication is not possible.

- **Remote Password Change authentication:** This type of authentication allows a user to change a forgotten password during the login process with the help of authorized personnel over the phone. This is also the basis for remotely unlocking a locked user account.

- **Smart card authentication:** Authentication mechanism employed by the TOE that utilizes smart cards to store credentials for the user that can only be accessed with a PIN, known only to the owner of the card.

- **System Administrator:** The highest authorization level in the administration of the TOE. This role can: create and administer profiles, configure system settings, add and remove administrators and users, configure settings for administrators and users, and provide remote assistance to users who are locked out or have forgotten their passwords.

- **System Area:** A protected area on each partition where TOE-specific security information is stored. The System Area is hidden from the OS and is under TOE control.

- **User Key (K_u):** Symmetric encryption key that is used to decrypt the Partition Key.

- **Users:** Any external user that interacts with the TOE.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] Check Point Endpoint Security Full Disk Encryption, Pointsec PC 6.3.1 Final Proprietary ETR – Part 2, Version 2.0 dated 2 July 2009 and Supplemental Team Test Report, Version 1.0, 11 June 2009.

[6] Check Point Endpoint Security Full Disk Encryption, Pointsec PC 6.3.1 Non-Proprietary ETR – Part 1, Version 1.0, 2 July 2009.

[7] Check Point Endpoint Security Full Disk Encryption Security Target, Version 2.4, 6/22/2009.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.