National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Pointsec Mobile Technologies, Inc.
Pointsec PC 4.3

Report Number: CCEVS-VR-04-0057

Dated: 28 January 2004

Version: 4.0

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

Donald Phillips, Lead Validator, Mitretek Systems

Common Criteria Testing Laboratory

Science Applications International Corporation

Columbia, MD

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Pointsec PC 4.3. It presents the evaluation results, their justifications, and the conformance results. This validation report 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 evaluation was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory, and was completed during January 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by SAIC. The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL4.**

The TOE, Pointsec PC 4.3, is a centrally administered, whole disk encryption and mandatory access control product for use on computers (laptops, desktops, or workstations) running Microsoft Windows operating systems. Mandatory access control is provided at the startup of the computer, prior to the loading of the operating system, requiring a successful authentication before the operating system is allowed to boot. Multiple user authentication mechanisms are supported, including fixed passwords, dynamic/challenge response authentication, smart cards, and remote help.

The primary security features for the Pointsec PC 4.3 are:

- **Access Control**: Secures desktops, workstations, and laptop from unauthorized access, using the combination of boot protection and full hard disk encryption, ensuring that unauthorized users are unable to access information on an encrypted device, either from available files, erased files, or temporary files.
- **Auditing**: 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.
- **Cryptographic Support**: The TOE's cryptographic functionality is based upon code that has been certified as meeting the requirements of FIPS 140-1 Level 1. Cryptographic keys are generated, accessed, protected, and destroyed in accordance with requirements defined by FIPS 140-1 Level 1. Additionally, the TOE supports important cryptographic operations such as data and key encryption/decryption.
- **Fault tolerance**: When a PC with Pointsec installed loses contact with the Pointsec Distribution Server, the TOE provides the administrator with the capability to identify an additional three Pointsec Distribution Servers for redundancy.
- **Identification and authentication**: The TOE provides a flexible suite of five authentication mechanisms, enabling the administrator to assign appropriate authentication requirements for the intended environment.

- **Security Management**: The TOE provides a number of interfaces to manage the configuration and implementation of the various policies enforced by the TOE.
- **Self –Protection**: Pointsec PC implements a set of security mechanisms to ensure that other security functions such as access control cannot be bypassed and that the security functions themselves cannot be tampered with. Additionally, mechanisms such as cryptographic self-tests have been implemented to ensure that important cryptographic functions are always operating correctly.
- **Trusted path**: The TOE provides a mechanism to ensure that users are communicating directly with the TOE during initial authentication.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST) for an EAL4 evaluation. Therefore, the validation team concludes that the SAIC CCTL findings are accurate, the conclusions justified.

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL 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;
- 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
Target of Evaluation	Pointsec PC Version 4.3
Protection Profile	Not applicable
Security Target	*Pointsec PC 4.3 Security Target ST Version 1.08 12 January 2004*
Evaluation Technical Report	*Evaluation Technical Report for Pointsec PC 4.3;* Version 1.0, January 9, 2004
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Pointsec Mobile Technologies, Inc.
Developer	Pointsec Mobile Technologies, Inc.
Evaluators	SAIC, Columbia, MD
Validators	Donald Phillips, Lead, Mitretek Systems

3. SECURITY POLICY

The TOE provides that users of the system shall be held accountable for their security relevant actions within the systems. The TOE must provide authorized administrators with utilities to effectively manage the security functions of the TOE. The TOE also ensures that cryptographic keys will be generated, accessed, protected, and destroyed in accordance with requirements defined by FIPS 140-1 Level 1. All cryptographic operation performed by the TOE will be compliant with FIPS 46-3 (3DES) and FIPS 197 (AES).

Only those users who have been authorized access to information with the TOE boundary may access the system. The TOE must have the ability to protect system data in transmission between distributed parts of the protected system. The TOE also must ensure that access control functions continue to operate if systems lose communications with central administration servers.

4. ASSUMPTIONS

4.1 Personnel Assumptions

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- Authorized TOE users and administrators are trusted to follow the guidance provided for the secure operation of the TOE.

4.2 Physical Assumptions

- The TOE’s IT environment will provide a reliable time source to enable the TOE to timestamp audit records.

- The TOE’s IT environment will provide a distribution server for the management of the TOE client software. This server provides installed PCs with a central point for storage of installation files, recovery files, update profiles, and software updates.

4.3 System Assumptions

- The system personnel maintain the 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 for the purposes of providing Remote Help authentication to authorized TOE users.

5. ARCHITECTURAL INFORMATION

Since the TOE is a software product, its physical boundary is defined by the files and information stored on the computer where it is installed. The TOE can be installed on any x86 compatible computer running Microsoft Windows 2000 or Windows XP. Due to the nature of the TOE's security functions, the underlying OS does not prohibit or interfere with the protection provided by the TOE. These functions are implemented uniformly across all listed OS platforms.

The Pointsec workstation or laptop will also communicate with the Pointsec Distribution Server, as depicted in Figure 1, below. This server provides member workstations/laptops with a central point for storage of installation files, recovery files, update profiles, and software updates. No components of the TOE are installed on the server as all communications are initiated from the workstation. The only requirement for this server is that it be accessible through network communications to the workstation using normal file share access, and not protocols such as ftp or http. All security related files are encrypted before they are stored on the server. Access to the server itself is configured through the server.

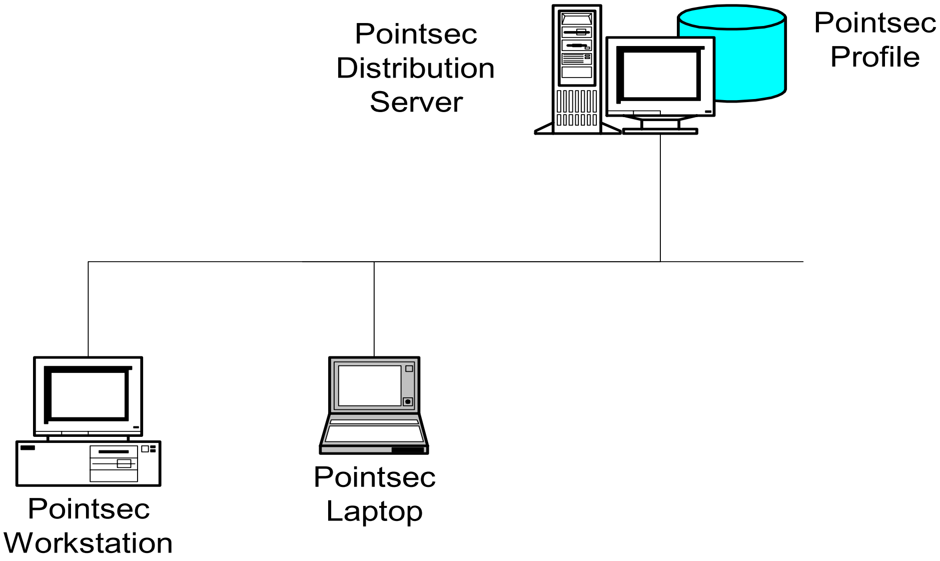

Figure 1

6. DOCUMENTATION

Design documentation

Document	Version	Date
Pointsec PC 4.3 Functional Specification	version 0.7	11/25/2003
Pointsec PC 4.3 High Level Design	version 0.7	12/08/2003

Pointsec PC 4.3 Low level Design	version 0.8	12/16/2003
Pointsec PC 4.3 TOE Security Policy Model – Informal	version 1.61	08/18/2003
Representation Correspondence	embedded in each design	

Guidance documentation

Document	Version	Date
Pointsec PC 4.3 Administrator’s Guide,	PA5	01/2004
Pointsec CBT for PC –Administrator		
Pointsec User CBT		

Configuration Management and Lifecycle documentation

Document	Version	Date
Pointsec Configuration Management Manual	version PA5	1/8/2004
Pointsec Change Control Process	version PA3	11/19/2003
Pointsec Building a Release	version 6	11/18/2003
Pointsec Bug Analyze and Correction Process	version PA4	11/19/2003
Pointsec Software Versioning and Release System	version PA5	3/28/2003
Software Development Process	PA4	11/19/2003
Dev Security	version 4	12/18/2003
Sundsval Physical Security	version 2	06/30/03
Sundsval Network	version 1	12/2002
Pointsec PC 4.3 Assurance Life Cycle	version .4	12/3/2003
Guidelines for Employment	version 0.2	
CD video evidence		

Delivery and Operation documentation

Document	Version	Date
Pointsec Software Product Delivery Manual	version 1.4	12/19/2003

Pointsec PC 4.3 Installation Guide	version PA2	01/2004

Test documentation

Document	Version	Date
Pointsec PC 4.3 Test Plan	version PA3	1/5/2004
Pointsec PC 4.3 Test Report	version 4	1/5/2004
Test Cases		

Vulnerability Assessment documentation

Document	Version	Date
Pointsec Vulnerability Analysis	version PA2	12/17/2003
Pointsec PC 4.3 Vulnerability – Strength of Function	version 1.4	9/30/2003
Pointsec PC 4.3 Misuse Analysis	version PA2	1/9/2004

Security Target

Document	Version	Date
Pointsec PC 4.3 Security Target	1.08	01/12/2004

7. IT PRODUCT TESTING

7.1 Developer Testing

The developer's approach to security testing is essentially focused on the testing of the interfaces. For each TFSI, security checks and effects are identified, and tests devised for each. Test documentation includes a high-level test plan that describes the philosophy of testing, and provides a mapping between the system components and specific test suites.

Prior to testing, the evaluation team verified that the TOE was as identified in the ST, and then proceeded to install and configure the TOE as described in the administrator guidance documentation. The following evaluation test configurations were installed to comply with the developers test procedures:

Hardware: The following hardware is used to create the test configuration.

- 3 Standard PC-computer laptop or desktop machines (x86 architecture)
- Smart cards and reader

- Tokens
- Floppy disks
- 1 6-port hub
- Ethernet Network cables

Software: The following software is required for the test configuration

- Windows 2000
- Windows XP
- Pointsec PC 4.3
- A DOS 6.22 bootable floppy disk

7.2 Evaluator Testing

The evaluation team applied each EAL4 ATE CEM work units. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security function as described in the functional specification and high-level design specification. The evaluation team performed a sample of the vendor test suite, and devised and independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The evaluation team tested the TOE Security Functional Interfaces (TFSI), which are listed below.

- Secure Audit
- Identification and Authentication
- User Data Protection

The evaluation team did not identify functional test for the following security functions. The evaluation team acknowledged that the vendor-supplied tests were sufficient to demonstrate the security functionality.

- Security Management
- TSF Protection
- Resource Utilization
- Trusted Path / Channels

8. EVALUATED CONFIGURATION

The evaluated configuration consists of the Pointsec PC Version 4.3 and the components are identified as the Pointsec PC 4.3 installed on Windows 2000 professional or Windows XP Platform

(**Note:** *Both operating systems were not tested with a specific patch build. The administrator is not required to perform a patch upgrade due to the security features built into the product.*)

9. RESULTS OF THE EVALUATION[1]

The evaluation team determined the product to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 4**. This implies that the product satisfies the security technical requirements specified in *Pointsec PC 4.3 Security Target Version 1.08 Release Date: January 12, 2004.*

10. EVALUATOR COMMENTS

There are no Evaluator Comments.

11. SECURITY TARGET

The ST, *Pointsec PC 4.3 Security Target Version 1.08, January 12, 2004* is included here by reference.

[1] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13. BIBLIOGRAPHY

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

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

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

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

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

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

[7] Pointsec PC 4.3 Security Target Version: 1.08, dated 12 January 2004

[8] Evaluation Technical Report, for Pointsec PC 4.3 Part 1 (Non Proprietary), 9 January 2004

[9] Evaluation Technical Report, for Pointsec PC 4.3 Version 1.0 Part 2 (SAIC and Pointsec Proprietary) 9 January 2004.

[10] Evaluation Team Test Plan for Pointsec PC 4.3 – EAL4 (Proprietary), Version 3.0, 8 January 2004.