Certification Report

EAL 4+ Evaluation of TNM v3.4 Software with CEP 10 VSE, CEP 100 VSE, CEP 1000 VSE, and CEP 10G VSE running CEP v2.1.1 Firmware

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-165-CR
Version: 1.0
Date: 18 December 2012
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI Security Evaluation and Test Facility.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 18 December 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

TNM v3.4 Software with CEP 10 VSE, CEP 100 VSE, CEP 1000 VSE, and CEP 10G VSE running CEP v2.1.1 Firmware (hereafter referred to as Certes TNM v3.4 and CEP v2.1.1), from Certes Networks, Inc, is the Target of Evaluation for this Evaluation Assurance Level 4 augmented evaluation.

Certes TNM v3.4 and CEP v2.1.1 consists of the Certes Enforcement Point (CEP) appliance hardware and appliance software and the TrustNet Manager (TNM) software-only management interface. The TOE is a custom-built hardware encryption appliance, configured and managed using custom-written application software. The TOE provides Layer 2 Ethernet frame encryption and Layer 3 IP packet encryption, encryption keys required for the encryption, and GUIs and Command Line Interfaces (CLI) for the management of its functionality. CEPs are the policy enforcement points. According to the policies received, CEPs can encrypt and decrypt traffic, send traffic in the clear, or drop traffic.

CGI Security Evaluation and Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 22 November 2012 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Certes TNM v3.4 and CEP v2.1.1, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Certes TNM v3.4 and CEP v2.1.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is TNM v3.4 Software with CEP 10 VSE, CEP 100 VSE, CEP 1000 VSE, and CEP 10G VSE running CEP v2.1.1 Firmware (hereafter referred to as Certes TNM v3.4 and CEP v2.1.1), from Certes Networks, Inc.

2 TOE Description

Certes TNM v3.4 and CEP v2.1.1 consists of the Certes Enforcement Point (CEP) appliance hardware and appliance software and the TrustNet Manager (TNM) software-only management interface. The TOE is a custom-built hardware encryption appliance, configured and managed using custom-written application software. The TOE provides Layer 2 Ethernet frame encryption and Layer 3 IP packet encryption, encryption keys required for the encryption, and GUIs and Command Line Interfaces (CLI) for the management of its functionality. CEPs are the policy enforcement points. According to the policies received, CEPs can encrypt and decrypt traffic, send traffic in the clear, or drop traffic. The CEP can be managed by authorized administrators via the Web GUI or directly via CLI commands. Through the GUI into TrustNet Manager, an administrator can configure and manage multiple appliances from a single centralized location. In addition, security policies defining how and where the encryption will take place can be created.

A detailed description of the Certes TNM v3.4 and CEP v2.1.1 architecture is found in Section 1.5 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Certes TNM v3.4 and CEP v2.1.1 is identified in Section 6 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
CEP10G VSE	1797
CEP10-R, CEP10 VSE and CEP10-C	1798
CEP100, CEP100 VSE, CEP100-XSA, CEP1000, CEP1000-DP and CEP1000 VSE	1799

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Certes TNM v3.4 and CEP v2.1.1:

Cryptographic Algorithm	Standard	Certificate #
Triple-DES (3DES)	FIPS 46-3	482, 673, 1195, 1258
Advanced Encryption Standard (AES)	FIPS 197	465, 762, 779, 1842, 1932
Rivest Shamir Adleman (RSA)	FIPS 186-2	998
Secure Hash Algorithm (SHA-1)	FIPS 180-2	1697
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	416, 417, 426, 1141, 1166

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: TNM v3.4 Software with CEP 10 VSE, CEP 100 VSE, CEP 1000 VSE, and CEP 10G VSE running CEP v2.1.1 Firmware
Version: 1.3
Date: 21 November 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Certes TNM v3.4 and CEP v2.1.1 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.

6 Security Policy

Certes TNM v3.4 and CEP v2.1.1 implements a role-based access control policy to control administrator access to the system, as well as an information flow control policy that applies a set of rules to Ethernet or IP traffic passing through the TOE. Depending on the operation identified in the security policy, the TOE will determine whether to pass user traffic in the clear, discard it, or apply encryption to it. Details of these security policies can be found in Section 6 of the ST.

In addition, Certes TNM v3.4 and CEP v2.1.1 implements policies pertaining to security audit, cryptographic support, identification and authentication, security management,

protection of the TSF, TOE access and trusted channels. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Certes TNM v3.4 and CEP v2.1.1 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system.
- The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
- The IT environment provides TrustNet Manager with the necessary reliable timestamps.
- The connections between the CEP and TNM management workstation, which is connected to TNM and TOE Environmental components, (the NTP, SNMP, and syslog servers) are all located within a controlled access facility on a secured network.

7.3 Clarification of Scope

Certes TNM v3.4 and CEP v2.1.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. Certes TNM v3.4 and CEP v2.1.1 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Certes TNM v3.4 and CEP v2.1.1 comprises the CEP10-VSE, CEP100-VSE, CEP1000-VSE, CEP10G-VSE Certes encryption appliances running the CEP v2.1.1 Software and the Linux Operating System (OS) and the TrustNet Manager v3.4 software.

The publication entitled *Certes Networks, Inc. TNM v3.4 Software with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware Guidance Documentation Supplement version 0.9* describes the procedures necessary to install and operate Certes TNM v3.4 and CEP v2.1.1 in its evaluated configuration.

9 Documentation

The Certes Networks, Inc documents provided to the consumer are as follows:

a. CEP VSE Certes Enforcement Point CLI User Guide, Version 2.1.1;

b. CEP VSE Certes Enforcement Point CLI Installation Guide, Version 2.1.1;

c. CEP VSE Release Note, Version 2.1.1;

d. TrustNet Manager User Guide, Version 3.4;

e. TrustNet Manager Installation Guide, Version 3.4;

f. TrustNet Manager Release Notes, Version 3.4; and

g. Certes Networks, Inc. TNM v3.4 Software with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware Guidance Documentation Supplement, Version 0.9.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Certes TNM v3.4 and CEP v2.1.1, including the following areas:

Development: The evaluators analyzed the Certes TNM v3.4 and CEP v2.1.1 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Certes TNM v3.4 and CEP v2.1.1 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that

security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Certes TNM v3.4 and CEP v2.1.1 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Certes TNM v3.4 and CEP v2.1.1 configuration management system and associated documentation was performed. The evaluators found that the Certes TNM v3.4 and CEP v2.1.1 configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Certes TNM v3.4 and CEP v2.1.1 during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Certes TNM v3.4 and CEP v2.1.1 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Certes Networks, Inc for Certes TNM v3.4 and CEP v2.1.1. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Certes TNM v3.4 and CEP v2.1.1. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to Certes TNM v3.4 and CEP v2.1.1 in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of CGI Security Evaluation and Test Facility test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Trusted Channel: The objective of this test goal is to demonstrate that CEP CLI traffic is protected with SSH;

c. Security Management: The objective of this test goal is to demonstrate that user accounts on CEP can be enabled and disabled and verifies that a user cannot log in to the CEP with the disabled account;

d. Administrator Roles TMN: The objective of this test goal is to demonstrate the privileges associated with different roles on TMN; and

e. Administrator Roles CEP: The objective of this test goal is to demonstrate the privileges associated with different roles on CEP.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Port Scanning. The objective of this test is to scan for open ports using nmap to compare against those that should be open;

b. Vulnerability Scanning. The objective of this test is to scan for known vulnerabilities with an open source vulnerability scanner;

c. Session Fixation. The objective of this test is to test the TNM web user interface to verify that the session ID cannot be determined by an attacker and whether the session ID is randomly generated;

d. Cross-Site Request Forgery .The objective of this test is to test the TNM web user interface to verify whether the TMN web user interface is susceptible to Cross-Site Request Forgery;

e. SQL and XSS: The objective of this test is to test the TNM web user interface to verify whether it is susceptible to SQL injection attacks and XSS attacks; and

f. SNMP: The objective of this test is to test the SNMP agent on CEP to verify that it should not present itself as an unmanaged/undocumented interface to the CEP.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Certes TNM v3.4 and CEP v2.1.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at CGI Security Evaluation and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Certes TNM v3.4 and CEP v2.1.1 behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

It is strongly recommended that the end customer shall consult ST section 1.5.3 and the Guidance Documentation Supplement to understand the evaluation configuration so that the TOE shall be configured in an evaluated and secure way.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3DES	Triple-Des
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEP	Certes Enforcement Point
CLI	Command Line Interface
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Keyed-Hash Message Authentication Code
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NTP	Network Time Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
RSA	Rivest Shamir Adleman
SHA-1	Secure Hash Algoritm
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
ST	Security Target
TNM	TrustNet Manager
TOE	Target of Evaluation
VSE	Variable Speed Encryptors
XSS	Cross Site Scripting

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Certes Networks, Inc. TNM v3.4 Software with CEP 10 VSE, CEP 100 VSE, CEP 1000 VSE, and CEP 10G VSE running CEP v2.1.1 Firmware, 1.4, 14 December 2012 Security Target.

e. Certes Networks, Inc TNM v3.4 Software with CEP 10 VSE, CEP 100 VSE, CEP 1000 VSE, and CEP 10G VSE running CEP v2.1.1 Firmware Common Criteria EAL4+ Evaluation Technical Report version 1.3, 14 December 2012.