Certification Report

EAL 2+ Evaluation of

Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet G2 Gateway product

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-67-CR
Version: 1.0
Date: 10 February 2009
Pagination: i to iii, 1 to 10

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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. 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 Standard 17025, 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 EWA-Canada located in Ottawa, Ontario.

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 10 February 2009, 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 at: http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/.

This certification report makes reference to the following trademarked names:

- Microsoft and Windows, which are registered trademarks of Microsoft Corporation.

TABLE OF CONTENTS

Executive Summary

Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product, hereafter referred to as the TNG 2E2 IA, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

TNG 2E2 IA is a gateway that connects integrated digital voice and data systems. TNG 2E2 IA includes both the gateway itself, and the separate management console. TNG 2E2 IA incorporates FIPS 140-2 validated encryption to secure Administrator communications.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 9 January 2009 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 the TNG 2E2 IA, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic flaw remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the TNG 2E2 IA evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[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.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is the Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet G2 Gateway product, hereafter referred to as the TNG 2E2 IA.

2 TOE Description

TNG 2E2 IA is a gateway that connects integrated digital voice and data systems. TNG 2E2 IA includes both the gateway itself, and the separate management console. TNG 2E2 IA incorporates FIPS 140-2 validated encryption to secure Administrator communications.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for TNG 2E2 IA is identified in Section 5 of the Security Target (ST).

Testing of the cryptographic algorithm implementations was accomplished under the Cryptographic Algorithm Validation Program (CAVP). The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in TNG 2E2 IA:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197, Advanced Encryption Standard (AES)	916
Secure Hash Algorithm (SHA-1)	FIPS 180-2, Secure Hash Standard	903

4 Security Target

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

Title: Security Target for the Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product
Version: 0.41
Date: 5 January 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

TNG 2E2 IA 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 2 augmented, containing all the security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.1 - Basic Flaw Remediation.

6 Security Policy

TNG 2E2 IA implements the Unauthenticated Information Flow and the Authenticated User Access Control security policies.

Unauthenticated Information Flow. The subjects under control of this policy are the TOE interfaces that connect to unauthenticated end-users. Traffic flowing between interfaces is controlled according to the policy rules and the traffic attributes. The policy is described further in Section 2.4 of the ST.

Authenticated User Access Control. This policy provides a role-based access control capability that defines tasks that are allowed to be performed by Administrators. This policy is described further in Section 2.4 of the ST.

In addition, TNG 2E2 IA implements administration and security management, audit, cryptography, TOE self-protection, trusted channel, and trusted path policies. Further details on these security policies are found in Section 2.3.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of TNG 2E2 IA 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 TNG 2E2 IA.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

a. The administrators will be competent and will adhere to the applicable TOE guidance; however they are capable of error.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.

b. The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.

c. It is assumed that information cannot flow between the connected networks unless it passes through the TOE.

d. There are no general-purpose computing or storage repository capabilities available on the TNG Headquarters (HQ) portion of the TOE.

e. It is assumed that the maintenance port on the TNG (HQ) portion of the TOE will not be used while the TNG (HQ) is in operational service.

f. It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

7.3 Clarification of Scope

TNG 2E2 IA provides a level of protection that is appropriate in environments where TNG 2E2 IA access is restricted to authorized personnel.

8 Architectural Information

TNG 2E2 IA comprises two main components: the TNG Equipment Management System (TEMS) and the TNG (HQ) gateway.

The TEMS is a software application that provides the means for Administrators to configure, control, and monitor the separate TNG (HQ) gateway. The TEMS runs on a Panasonic CF-29 Toughbook. The Toughbook and its operating system and applications are not included in the evaluation.

The TNG (HQ) provides voice and data gateway facilities between networks. The evaluated TNG (HQ) comprises the Objective Network Access Units (oNAUs): TNG (Core), TNG (ISDN), and TNG (DTMF). Additional oNAUs (e.g. TNG (Fw) which is a firewall) may be incorporated into the TNG (HQ) but are not included in the evaluation.

The Toughbook (TEMS application) connects to the TNG (HQ) using Ethernet. FIPS 140-2 validated encryption is used to secure communications between the TEMS and the TNG (HQ).

Further details about the system architecture are proprietary to the developer, and are not provided in this report.

9 Evaluated Configuration

The TOE is identified as:

- TNG Equipment Management System (TEMS) – Version TNG SysMan Release 2E2 IA; and

- TNG Headquarters (HQ) – Firmware Version 2E2 IA, and Hardware Versions CORE: 723975-908, ISDN: 723974-908, and DTMF: 723973-903.

The workstation supporting the TEMS comprises a Panasonic CF-29 Toughbook with:

- Microsoft Windows 2000 Service Pack 4 with hotfixes and patches;
- HP ProtectTools Authentication Services;
- TNG Equipment Management Applications (TEMS and TNG (Fw));
- SSH Software & Certification Authority Key Material; and
- Microsoft .NET Framework version 1.1 & 2.0.

10 Documentation

The GD Canada documents provided to the consumer are as follows:

a. Lesson Plan Set up and Maintain the Tactical Network-layer Gateway 682283, 9 January 2007; and

b. TNG Equipment Management Program Help 8322C-1, 30 July 2008.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the TNG, including the following areas:

Configuration management: An analysis of the TNG 2E2 IA configuration management system and associated documentation was performed. The evaluators found that the TNG 2E2 IA configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of TNG 2E2 IA during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration. The developer's delivery system and procedures were observed during a site visit, and found to be complete and secure.

Design documentation: The evaluators analysed the TNG 2E2 IA functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the TNG 2E2 IA administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by GD Canada for the TNG 2E2 IA. 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 TNG 2E2 IA ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for TNG 2E2 IA and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessing 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].

GD Canada employs a rigorous testing process that tests the changes and fixes in each release of TNG 2E2 IA. Comprehensive regression testing is conducted for all releases.

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation,

[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.

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 was the following list of EWA-Canada 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. Initialization. The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

c. Identification and Authentication. The objective of this test goal is to ensure that the identification and authentication requirements have been met;

d. Audit. The objective of this test goal is to ensure that the audit data is recorded and can be viewed; and

e. Users and Roles. The objective of this test goal is to ensure the users and roles functionality is correct.

12.3 Independent Penetration Testing

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

a. Host Scanning. Nmap and ping were used to scan the address range to identify “live” hosts for use as potential targets the other tests.

b. Port Scanning. Nmap and netcat were used to scan TCP and UDP ports on the target systems to identify which services were available.

c. TCP Fingerprinting. Nmap was used to scan the targets in an attempt to identify the remote operating system and version.

d. Banner Grabbing. Nmap, netcat and telnet were used to connect to the targets in an attempt to identify the service listening on a given port and its version.

e. Vulnerability Scanning. Nessus and Retina were used to conduct comprehensive vulnerability scans of the target systems.

f. Verification of Vulnerabilities. The vulnerabilities that were identified by the automated and semi-automated tools were verified and an attempt was made to uncover other vulnerabilities and issues that were not reported by the automated tools.

g. Security Restrictions Bypassing. Probing of the TOE was done in an attempt to bypass security restrictions. This was achieved by verifying and testing the level of hardening on the Toughbook and TNG (HQ) operating systems.

h. Tampering. Tampering of the TOE was done in an attempt to see if the TOE could be misused by its users. This was achieved by verifying and testing the level of hardening on the Toughbook and TNG (HQ) operating systems.

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

12.4 Conduct of Testing

TNG 2E2 IA was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the GD Canada facility in Calgary, Alberta. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the TNG 2E2 IA behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 augmented level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

GD Canada has a mature and comprehensive set of Operations Standard Procedures (OSPs) that fully define configuration management, requirements management, and baseline management.

GD Canada has a complete, thorough CM program encompassing the personnel, processes and resources required to maintain configuration management during the development, integration, testing, production, delivery and support phases of the TNG 2E2 IA project.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DTMF	Dual Tone Multi-Frequency
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISDN	Integrated Service Digital Network
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
GDC	General Dynamics Canada
GD Canada	General Dynamics Canada
oNAU	Objective Network Access Unit
OSP	Operations Standard Procedures
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TNG	Tactical Network-layer Gateway
TOE	Target of Evaluation
TNG (Core)	Tactical Network-layer Gateway Core
TNG (Fw)	Tactical Network-layer Gateway Firewall
TNG (HQ)	Tactical Network-layer Gateway Headquarters
TEMS	TNG Equipment Management System

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.0, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. Security Target for the Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product, Revision No. 0.41, 5 January 2009.

e. Evaluation Technical Report (ETR) for EAL 2+ Common Criteria Evaluation of the Tactical Network-layer Gateway v1.0: a GD Canada MESHnet G2 Gateway product, Evaluation Number: 383-4-67, Document No. 1531-000-D002, Version 2.4, 9 January 2009.