Certification Report

EAL 4+ Evaluation of QNX Neutrino® Secure Kernel v6.4.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-95-CR
Version: 1.0
Date: 25 March 2009
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 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 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 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 25 March 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:

- QNX® and QNX Neutrino® are registered trademarks of QNX® Software Systems.

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **3**

2 TOE Description **3**

3 Evaluated Security Functionality **3**

4 Security Target **3**

5 Common Criteria Conformance **3**

6 Security Policy **4**

7 Assumptions and Clarification of Scope **4**

7.1 SECURE USAGE ASSUMPTIONS 4
7.2 ENVIRONMENTAL ASSUMPTIONS 5
7.3 CLARIFICATION OF SCOPE 5

8 Architectural Information **5**

9 Evaluated Configuration **5**

10 Documentation **6**

11 Evaluation Analysis Activities **6**

12 ITS Product Testing **7**

12.1 ASSESSING DEVELOPER TESTS 8
12.2 INDEPENDENT FUNCTIONAL TESTING 8
12.3 INDEPENDENT PENETRATION TESTING 9
12.4 CONDUCT OF TESTING 9
12.5 TESTING RESULTS 9

13 Results of the Evaluation **10**

14 Evaluator Comments, Observations and Recommendations **10**

15 Acronyms, Abbreviations and Initializations **10**

16 References **11**

Executive Summary

The QNX Neutrino® Secure Kernel from QNX Software Systems, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

The QNX Neutrino® Secure Kernel v6.4.0 provides the microkernel for the QNX Neutrino® Realtime Operating System. QNX Neutrino® Secure Kernel v6.4.0 provides a memory protected microkernel architecture for reliable, scalable and realtime performance in embedded applications. The QNX Neutrino® Secure Kernel v6.4.0 operates as a self-contained, protected microkernel within the QNX Neutrino® RTOS. This allows the secure kernel to be used as a core system building block in a wide variety of operating system technologies.

In addition to its POSIX-compliant features, the QNX Neutrino® Secure Kernel v6.4.0 implements an optional scheduling algorithm. The scheduling algorithm allows partitions to be created with a defined budget (percentage) of CPU cycles. Processes and threads are assigned to partitions and under conditions of heavy CPU load each partition is guaranteed to receive its assigned share of CPU cycles regardless of the priority of the processes/threads assigned to the partition. The scheduler is adaptive in that under normal load conditions unused CPU cycles from one partition are allocated to other partitions running processes/threads of higher priority.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 13 March 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 QNX Neutrino® Secure Kernel, 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 4 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*

[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.

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 QNX Neutrino® Secure Kernel 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the QNX Neutrino® Secure Kernel, from QNX Software Systems.

2 TOE Description

The QNX Neutrino® Secure Kernel v6.4.0 provides the microkernel for the QNX Neutrino® Realtime Operating System. QNX Neutrino® Secure Kernel v6.4.0 provides a memory protected microkernel architecture for reliable, scalable and realtime performance in embedded applications. The QNX Neutrino® Secure Kernel v6.4.0 operates as a self-contained, protected microkernel within the QNX Neutrino® RTOS. This allows the secure kernel to be used as a core system building block in a wide variety of operating system technologies.

In addition to its POSIX-compliant features, the QNX Neutrino® Secure Kernel v6.4.0 implements an optional scheduling algorithm. The scheduling algorithm allows partitions to be created with a defined budget (percentage) of CPU cycles. Processes and threads are assigned to partitions and under conditions of heavy CPU load each partition is guaranteed to receive its assigned share of CPU cycles regardless of the priority of the processes/threads assigned to the partition. The scheduler is adaptive in that under normal load conditions unused CPU cycles from one partition are allocated to other partitions running processes/threads of higher priority.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the QNX Neutrino® Secure Kernel is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title:	QNX® Software Systems, QNX Neutrino® Secure Kernel v6.4 Security Target
Version:	Document Version 1.1
Date:	15 December 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*.

The QNX Neutrino® Secure Kernel 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, with all the security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1.

6 Security Policy

The QNX Neutrino® Secure Kernel implements an Access Control Security Functional Policy which governs the assignment of CPU resources (cycles) to executing threads based both on the priority assigned to the thread and the adaptive partition to which the thread is assigned.

The QNX Neutrino® Secure Kernel also implements an Information Flow Control Security Functional Policy which governs the creation and subsequent access to shared memory resources based upon both the permissions of the creating/accessing thread and the permissions assigned to the shared memory area at creation.

Details of the Access Control and Information Flow Control security policies can be found in Section 5 of the ST.

In addition to the named security policies listed above, QNX Neutrino® Secure Kernel also implements policies pertaining to process/thread identification, security management, residual information protection and protection of the TOE, including fault tolerance, priority of service and CPU usage quotas. Further details on these security policies are found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the QNX Neutrino® Secure Kernel product 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 QNX Neutrino® Secure Kernel.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Competent, trusted and trained administrative staff are assigned to install, configure and operate the QNX Neutrino® Secure Kernel; and

- Staff assigned to write processes and threads for execution by the TOE are non-hostile, appropriately trained and adhere to all appropriate guidance.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security measures commensurate with the value of assets protected by the TOE exist for the environment in which the TOE is hosted

7.3 Clarification of Scope

Users of QNX Neutrino® Secure Kernel should note that QNX Neutrino® Secure Kernel includes only the QNX Neutrino® Secure Kernel which consists of the procnto system process and its associated C library. As such the TOE does not constitute a complete product intended for consumer use, but rather consists of a secure kernel which product developers may use in order to create a wide variety of commercial products. Users of QNX Neutrino® Secure Kernel are therefore cautioned that the ultimate security of commercial products based upon the TOE may be highly dependent upon the additional features added to the TOE in order to create an end user product. In particular, users of QNX Neutrino® Secure Kernel should note that it does not include any audit capabilities, nor does it include any drivers, files systems or networking capabilities.

8 Architectural Information

The TOE consists solely of the compiled QNX Neutrino Realtime Operating System microkernel which encompasses the Procnto Subsystem (compiled and executed as the procnto system process) and the C Library Subsystem (the compiled lib/c C-Language library). The lib/c subsystem provides the external interface to which other external applications (including other OS components and user applications) can link.

9 Evaluated Configuration

The evaluated configuration of the TOE consists of the QNX Neutrino® Secure Kernel v6.4.0 running on the following processor families:

a. ARM9;

b. ARM11; and

c. x86 Multicore.

As described in the previous section, the TOE boundary encompasses only the procnto system process and the compiled lib/c C-language library. All other components fall outside the TOE boundary in the IT environment. These include all hardware items such as CPU boards, power supplies and video displays. The IT environment also includes all of the

software components required to create a functional operating system including device drivers, files systems, networking and user applications. The TOE was tested by compiling the QNX Neutrino® Realtime Operating System v6.4.0 with the QNX Neutrino® Secure Kernel v6.4.0 and the optional adaptive partitioning scheduler as described in the QNX Neutrino® Secure Kernel 6.4.0 Release Notes Section 10.e.

10 Documentation

The QSS documents provided to the consumer are as follows:

- QNX Neutrino® RTOS: Getting Started with QNX Neutrino®, A Guide for Realtime Programmers by Rob Krten;
- QNX Neutrino® RTOS User's Guide, for release 6.4 or later;
- QNX Neutrino® RTOS System Architecture, for release 6.4.0;
- QNX Neutrino® Secure Kernel 6.4.0, Release Notes;
- QNX Neutrino® Secure Kernel 6.4.0, Installation Note;
- QNX Neutrino® RTOS Adaptive Partitioning User's Guide, for QNX Neutrino® 6.4.0; and
- QNX Neutrino® Realtime Operating System Utilities Reference, for QNX Neutrino® 6.4.0.

In addition the QSS web site (http://qnx.com) provides access to a wide range of additional product documentation, including white papers and source code.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the QNX Neutrino® Secure Kernel, including the following areas:

Configuration management: An analysis of the QNX Neutrino® Secure Kernel configuration management system and associated documentation was performed. The evaluators found that the QNX Neutrino® Secure Kernel 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 the QNX Neutrino® Secure Kernel 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.

Design documentation: The evaluators analysed the QNX Neutrino® Secure Kernel functional specification, high-level design, low-level design, and a subset of the implementation representation. The evaluators 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 QNX Neutrino® Secure Kernel user and 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 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 QNX Neutrino® Secure Kernel 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 QSS for the QNX Neutrino® Secure Kernel. 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 examined the developer's vulnerability analysis for the QNX Neutrino® Secure Kernel 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 4 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].

QNX Software Systems employs a rigorous testing process for the QNX Neutrino® Secure Kernel. The automated testing process includes functional testing based upon product requirement documents as well as feature specific testing derived from the problem reporting system. Comprehensive regression testing is conducted for each candidate build of the product.

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The developer's test documentation demonstrated complete correspondence between the tests identified in the developer's test documentation and both the functional specification and high level design.

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, 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 approach was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to follow the developer's procedures for installation and configuration of QNX Neutrino® Secure Kernel in order to ensure that the tested version of QNX Neutrino® Secure Kernel is identical to the evaluated configuration described in the Security Target.

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

c. Resource Utilization: The objective of this test goal is to confirm that QNX Neutrino® Secure Kernel allocates CPU resources based on thread priority and that QNX Neutrino® Secure Kernel is also able to guarantee a specific percentage of CPU resources to the thread or threads running within an adaptive partition.

[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.

d. Protection of the TSF: The objective of this test goal is to confirm that the failure of a process or thread does not prevent the continued execution of other processes or threads.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, independent 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:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks

As a result of this analysis, a number of independent vulnerability and penetration test cases were developed and executed. Given the limited scope of the TOE boundary, the penetration tests focused on the area of direct attacks as this appeared to be the most likely area for vulnerabilities to be found.

The evaluator did not uncover any vulnerabilities which were not described in the developer's vulnerability analysis. The evaluator found that QNX Neutrino® Secure Kernel did not have any open ports. The evaluator also tested failure modes and was unable to place QNX Neutrino® Secure Kernel into an insecure state via a failure. The evaluator executed a denial of service attack (large process volume) and was unable to induce either failure or service degradation in QNX Neutrino® Secure Kernel.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment of QNX Neutrino® Secure Kernel.

12.4 Conduct of Testing

The QNX Neutrino® Secure Kernel was subjected to a suite of documented, independent functional and penetration tests. The testing took place both at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada and at the testing facilities of QNX® Software Systems. 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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the QNX Neutrino® Secure Kernel behaves as specified in its ST and functional specification.

13 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.

14 Evaluator Comments, Observations and Recommendations

QNX® Software Systems employs a full time Quality Manager and has implemented a comprehensive Quality System which permeates every aspect of the company from product conceptualization through development and extending into marketing, sales and support. The wide range of quality, safety, security and industrial certifications achieved by the company are clear evidence of the corporate commitment to the quality system.

QNX® Software Systems has also adopted a highly proactive approach to security within their products. The company has designated an individual within the development team to monitor the public security forums and act as the focal point for security issues related to QNX® Software Systems products. The company has a very active user community who are well supported by the company and are actively encouraged to provide security feedback to the development team. The evaluators were able to observe this process in operation during the evaluation as a user discovered security flaw was reported, recorded, tracked and corrected during the course of the evaluation.

The evaluators found the QNX® Software Systems documentation for the TOE to be of exceptional quality. The installation guidance was clear and precise. The user guidance was equally clear and included very frank and realistic sections describing security issues and decisions that users must make in order to implement a secure system using the TOE.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Standards Organization
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories

Acronym/Abbreviation/ Initialization	Description
	Canada
POSIX	Portable Operating System Interface for UNIX
QA	Quality Assurance
RTOS	Real Time Operating System
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) CCS-Guide-004, Version 1.1, Technical Oversight for TOE Evaluation.

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. **QNX**® Software Systems, QNX Neutrino® Secure Kernel v6.4 Security Target, Document Version 1.1, 15 December 2009.

e. Evaluation Technical Report (ETR) QNX Neutrino® Secure Kernel, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-95, Document No. 1576-000-D002, Version 1.4, 13 March 2009.