Certification Report

EAL 4+ Evaluation of nCipher nShield Family of Hardware Security Modules Firmware Version 2.33.60

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-82-CR
Version: 1.2
Date: 30 October 2009
Pagination: i to iv, 1 to 9

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 Information Technology 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 DOMUS IT Security Laboratory 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 or registered trademarks:

- nCipher, netHSM and nShield are trademarks or registered trademarks of nCipher Corporation Ltd.; and
- Windows is a registered trademark of Microsoft Corporation.

TABLE OF CONTENTS

Executive Summary

nCipher nShield Family of Hardware Security Modules Firmware Version 2.33.60 (hereafter referred to as nShield HSM Firmware), from nCipher Corporation Ltd., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

The TOE, nShield HSM Firmware, is the firmware executing on a dedicated PCI card. The firmware provides protection for the cryptographic keys used within computing platforms, managing cryptographic key generation, archiving, recovery and destruction and incorporates FIPS PUB 140-2 validated cryptography.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 17 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 nShield HSM Firmware, 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 *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 nShield HSM Firmware 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) 4 augmented evaluation is nCipher nShield Family of Hardware Security Modules Firmware Version 2.33.60 (hereafter referred to as nShield HSM Firmware), from nCipher Corporation Ltd..

2 TOE Description

The TOE, nShield HSM Firmware, is the firmware executing on a dedicated PCI card. The firmware provides protection for the cryptographic keys used within computing platforms, managing cryptographic key generation, archiving, recovery and destruction and incorporates FIPS PUB 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for nShield HSM Firmware is identified in Section 6 of the Security Target.

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

Cryptographic Module	**Certificate #**
nShield F3 4000, nShield F3 2000, nShield F3 2000 for netHSM, nShield F3 500 and nShield F3 500 for netHSM	*#965*
nShield F3 500, nShield F3 500 for NetHSM and nShield F3 10 PCI	*#966*
nShield F3 4000, nShield F3 2000, nShield F3 2000 for netHSM, nShield F3 500 and nShield F3 500 for netHSM	*#968*
nShield F3 500, nShield F3 500 for NetHSM and nShield F3 10 PCI	*#970*
nShield F2 500 and nShield F2 10 PCI	*#973*
nShield F2 4000, nShield F2 2000 and nShield F2 500	*#977*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in nShield HSM Firmware:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	#570
Advanced Encryption Standard (AES)	FIPS 197	#599
Rivest Shamir Adleman (RSA)	ANSI X9.31	#274
Secure Hash Algorithm (SHA-1)	FIPS 180-2	#648
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	#309
Random Number Generator (PRNG)	FIPS 186-2 Change Notice 1 SHA-1 and FIPS 186-2	#340

	RNG General Purpose RNG	
Digital Signature (DSA and ECDSA)	FIPS 186-2	#64,#233

4 Security Target

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

Title: nCipher nShield Family of Hardware Security Modules Firmware Version 2.33.60 Security Target
Version: 1.9
Date: 17 March 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.*

nShield HSM Firmware 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.1 – Basic Flaw Remediation.

6 Security Policy

nShield HSM Firmware implements a Cryptographic Operations and Key Management security policy to manage cryptographic key generation, archiving, recovery and destruction. Further details of this security policy are found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of nShield HSM Firmware 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 nShield HSM Firmware.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- The administrative users are assumed to be trusted and not careless, willfully negligent, or hostile. The administrative users must follow and abide by the instructions provided by the user guidance documentations.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- nShield HSM Firmware is assumed to be located in a physically secure location, with appropriate physical security measures.

7.3 Clarification of Scope

nShield HSM Firmware provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While nShield HSM Firmware is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone, nor could it provide complete protection against authorized key custodian intentionally or carelessly disclosing the secret information under their control.

NOTE: It should be noted here that the TOE is firmware only. This evaluation did not include any of the hardware platforms.

8 Architectural Information

nShield HSM Firmware is a firmware executing on a dedicated PCI card. The firmware comprises the six subsystems: Command Dispatch, nCore API, Crypto Mechanisms, Device Abstractions, Device Drivers, and Run-time Libraries.

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

9 Evaluated Configuration

The evaluated configuration for nShield HSM Firmware comprises firmware version 2.33.60cam1 in its default state running on the following hardware platforms:

- nShield PCI F3 500;
- nShield PCI F3 2000;
- nShield PCI F3 4000;

- nShield PCI F2 500;
- nShield PCI F2 2000;
- nShield PCI F2 4000;
- netHSM 500 (containing an nShield PCI F3 500); and,
- netHSM 2000 (containing an nShield PCI F3 2000).

10 Documentation

The nCipher Corporation Ltd. documents provided to the consumer are as follows:

- nShield User Guide (UNIX-based) version 6.2;
- netHSM User Guide (UNIX-based) version 6.3;
- nShield User Guide (Windows) version 6.2;
- netHSM User Guide (Windows) version 6.3;
- nCore API developer reference guide build 2.10.77;
- nShield QuickStart Guide (UNIX-based) version 3.2;
- nShield User Guide (UNIX-based) version 6.2;
- nShield QuickStart Guide (Microsoft Windows) version 3.2;
- nShield User Guide (Windows) version 6.2; and
- Hardware Installation Guide Version 3.0.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of nShield HSM Firmware, including the following areas:

Configuration management: An analysis of the nShield HSM Firmware configuration management system and associated documentation was performed. The evaluators found that the nShield HSM Firmware configuration items were clearly marked, and could be modified and controlled, and that the configuration management system supported generation of the TOE. 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 nShield HSM Firmware 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 nShield HSM Firmware functional specification, high-level design, low-level design, security policy model, and a subset of the implementation representation; 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 nShield HSM Firmware administrator and user 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 the nShield HSM Firmware 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 nCipher Corporation Ltd. for nShield HSM Firmware. 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 nShield HSM Firmware ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for nShield HSM Firmware 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 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 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, 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 DOMUS IT Security Laboratory test goals:

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

b. Cryptographic key management: The objective of these tests is to determine the TOE's ability to provide well managed cryptographic key generation, archiving, recovery and destruction.

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:

- Bypassing;
- Tampering; and
- Direct attacks.

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

[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.

12.4 Conduct of Testing

nShield HSM Firmware 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 DOMUS IT Security Laboratory. 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 nShield HSM Firmware 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

nCipher Corporation Ltd. provides comprehensive guidance documents for the installation, configuration and operation of nShield HSM Firmware.

nCipher Corporation Ltd. employs a rigorous testing process that tests all releases.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HSM	Hardware Security Modules
IT	Information Technology
ITSET	Information Technology Security Evaluation

Acronym/Abbreviation/ Initialization	Description
	and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2005-08-002, Version 2.3, August 2005.

c. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2005-08-003, Version 2.3, August 2005.

d. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2005-08-004, Version 2.3, August 2005.

e. nCipher nShield Family of Hardware Security Modules Firmware Version 2.33.60 Security Target, Version 1.9, 17 March 2009.

f. nCipher Corporation Ltd., nCipher nShield Family of Hardware Security Modules Firmware Version 2.33.60, Evaluation Technical Report, Version 1.3, 17 March 2009.