Maintenance Report

nCipher nShield ™ Family of Hardware Security Modules FirmWare Version 2.33.82

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-7-40-MR
Version:	1.0
Date:	June 15, 2009
Pagination:	1 to 2

1 Introduction

On 28 May 2008, DOMUS IT Security Laboratory submitted an Impact Analysis Report to the CCS Certification Body on behalf of nCipher Corporation Ltd., the developer of the nCipher nShield ^{TM} Family of Hardware Security Modules FirmWare Version 2.33.82 (hereafter referred to as the nShield HSM firmware) product. The Impact Analysis Report is intended to satisfy requirements outlined in version 1.0 of the Common Criteria document CCIMB-2004-02-009: Assurance Continuity: CCRA Requirements. In accordance with those requirements, the Impact Analysis Report (IAR) describes the changes made to nShield HSM firmware (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes to the TOE

The following characterizes the changes implemented in the nShield HSM firmware. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained. The changes in the nShield HSM firmware comprise bug fixes resulting from defects detected and resolved through the QA/test process as well as performance improvements to the cryptographic module. The crypto module validation is covered by FIPS 140-2 validation certificates numbers 1063, 1064 and 1065.

3 Description of Changes to the IT Environment

Changes to the IT Environment are permissible under assurance continuity provided that they do not change the certified TOE. A modified ST was provided which listed the updated software. nCipher Corporation subjected the TOE to complete regression testing. The changes to the IT Environment (product) include the addition of support for the PCIe interface as well as the following new hardware platforms supported by the TOE:

- nShield F3 6000e
- nShield F3 500e
- nShield F2 6000e
- nShield F2 500e
- nShield F3 1500e
- nShield F2 1500e

and a product name change.

4 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

5 Conclusions

All changes to the TOE were bug fixes and performance improvements. Through functional and regression testing of the nShield HSM firmware, assurance gained in the original TOE certification was maintained. As all of the changes to the TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

6 References

Assurance Continuity: CCRA Requirements, CCIMB-2004-02-009, version 1.0, February 2004

Technical Oversight for Assurance Continuity of a Certified TOE, version 1.2, October 2005

Certification Report EAL 4+ Evaluation of nCipher nShield^{tm} Family of Hardware Security Modules Firmware version 2.33.60