Certification Report

nShield Solo XC Hardware Security Module v12.60.15

Sponsor:	***Entrust*** **Minneapolis1187 Park Place** **Shakopee, MN 55379** **USA**
Developer:	***nCipher Security Limited (an Entrust company)*** **One Station Square** **Cambridge CB1 2GA** **UK**
Evaluation facility:	***Brightsight B.V*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-163968-CR2**
Report version:	**1**
Project number:	**163968_2**
Author(s):	**Denise Cater**
Date:	**17 March 2021**
Number of pages:	**12**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword **3**

Recognition of the certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **6**

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 6
2.4 Architectural Information 7
2.5 Documentation 8
2.6 IT Product Testing 8
2.7 Re-used evaluation results 9
2.8 Evaluated Configuration 10
2.9 Results of the Evaluation 10
2.10 Comments/Recommendations 10

3 Security Target **11**

4 Definitions **11**

5 Bibliography **12**

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the nShield Solo XC Hardware Security Module v12.60.15. The developer of the nShield Solo XC Hardware Security Module v12.60.15 is nCipher Security Limited located in Cambridge, UK. The sponsor of the evaluation and certification is Entrust, located in Shakopee, USA. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE can be used as a general purpose Cryptographic Module in a wide range of use cases, including, but not limited to, Trust Service Providers to provide a QSCD for Remote Server Signing.

The TOE is a general purpose Cryptographic Module which comes in a PCI express board form factor protected by a tamper resistant enclosure. It performs encryption, digital signing, and key management on behalf of an extensive range of commercial and custom-built applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenization, SSL/TLS, and code signing.

The nShield Solo XC HSM can also be embedded inside the nShield Connect XC, which is a network-attached appliance delivering cryptographic services as a shared network resource for distributed applications and virtual machines, giving organizations a highly secure solution for establishing physical and logical controls for server-based systems.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 15 November 2019. The re-evaluation also took place by Brightsight B.V. and was completed on 17 March 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are update of the firmware relating to extended/enhanced cryptographic functionality and associated updates to the guidance documentation.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the nShield Solo XC Hardware Security Module v12.60.15, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the nShield Solo XC Hardware Security Module v12.60.15 are advised to verify that their own environment is consistent with 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 provides sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw remediation) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the nShield Solo XC Hardware Security Module v12.60.15 from nCipher Security Limited located in Cambridge, UK.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	nShield Solo XC F2	nC3025E-000 rev 06
	nShield Solo XC F3	nC4035E-000 rev 06
	nShield Solo XC for nShield Connect XC	nC4335N-000 rev 06 This module is embedded in the nShield Connect XC appliance with model number NH2075-x or NH2089-x (where x is B, M or H)
Software	Solo XC firmware image	v12.60.15

To ensure secure usage a set of guidance documents is provided together with the nShield Solo XC Hardware Security Module v12.60.15. Details can be found in section 0 of this report.

2.2 Security Policy

The TOE implements key generation, key import/export and key agreement. It also provides cryptographic services including digital signature, encryption/decryption, message digest, message authentication and Random Number Generation. The supported algorithms and key sizes are specified in *[ST]* Table 2.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that EN 419221-5 Protection Profile [EN419221-5] claims the environment for the TOE protects against loss or theft of the TOE, deters and detects physical tampering, protects against attacks based on emanations of the TOE, and protects against unauthorised software and configuration changes on the TOE and the hardware appliance it is contained in ("OE.Env Protected operating environment").

The ST follows the PP and also claims OE.Env, thus the environment in which the TOE is used must ensure the above protection.

Any threats violating these objectives for the environment are not considered.

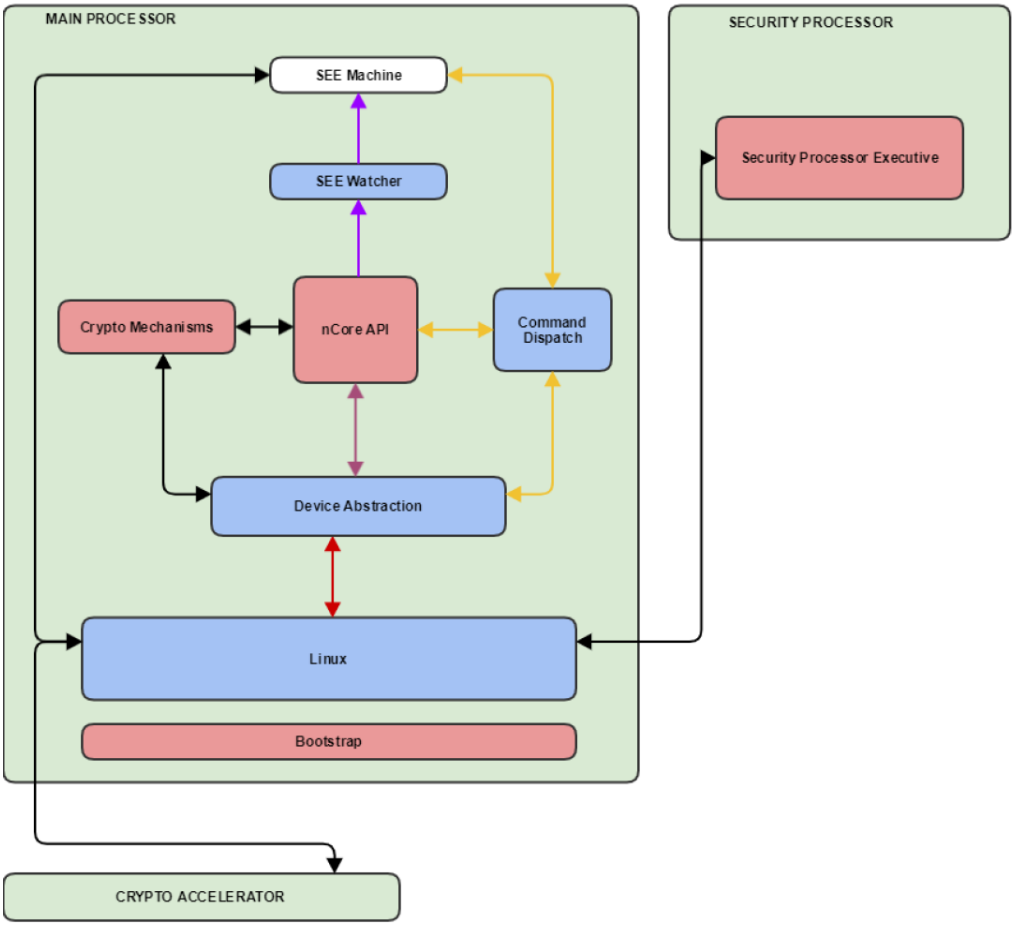
The TOE does not implement an optional trusted path to an external application therefore the SFR, FTP_TRP.1/External, which is marked as optional in the Protection Profile, has been removed in *[ST]*.

2.4 Architectural Information

The TOE supports two configurations as detailed in section 1.3.2 of *[ST].*

The TOE comes in a PCI express board form factor protected by a tamper resistant enclosure, and can also be embedded inside the nShield Connect XC, which is a network-attached appliance.

The logical boundary of the TOE comprises the firmware located inside the PCIe board, with the exception of embedded CodeSafe applications and is comprised of the following subsystems:



The TOE provides the following security features:

- Cryptographic functions, including digital signature, encryption/decryption, key agreement, message digest, message authentication, key generation,
- Random Number Generation,
- Secure key management,
- Secure logging,
- Physical tamper resistance meeting *[ISO 19790]* Level 3.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
nShield Solo XC Common Criteria Evaluated Configuration Guide	V1.1, dated Tuesday 16 March, 2021

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has performed extensive testing on functional specification, subsystem and SFR-enforcing module level. For each SFR the developer created an extensive set of automatic tests, testing positively and negatively. Crypto testing for the FCS_COP requirements are tested against two oracles the CAVS verification tool and the OpenSSL implementation. For all tests the log files were also collected, showing full coverage of the FAU_GEN requirements. All nCore commands over the PCIe TSFI are tested via the external nCore PCIe interface, the SEE system-calls are tested by executing a local application on the TOE.

Additionally the developer implemented a set of manual test cases focusing on internals of the TOE functionality and behaviour.

The combination of the automated tests, the manual tests and the hardware tests demonstrate the correct behaviour of all the TSFIs, with exception of the Clear Button and the Mode Switch. The functionality however of these TSFIs are tested by the developer using the nCore commands and were also the subject of independent evaluator testing.

During the baseline evaluation, the evaluator repeated all the tests of the following test sets: Ncoretest, Seccomp, Crypto Validation. This was performed on the developer development site. These test scenario tests all nCore functionality related to SFR-related actions as invoked by the host, cryptographic validation tests and test for syscalls within SEE machine, firmware downgrade/corruption tests and the tests for disabled nCore commands. The evaluator also assessed the developer test case against all the SFRs and noted there are few SFRs that are not fully tested. The evaluator defined a few complementary tests to validate the TOE behaviours that were not covered by the developer tests.

In addition the refinements of ATE_IND.2 specified in *[EN419221-5]* were addressed during evaluator independent testing, namely:

(1) The evaluator shall execute the electronic signature and electronic seal operations provided by the TOE and shall confirm that the signatures and seals returned by the TOE correspond to the correct DTBS.
(2) If software and/or firmware updates are supported by the TOE then the evaluator shall carry out tests to ensure that only updates with valid digital signatures can be installed on the TOE.

During this re-evaluation, in addition to repeating a sample of the developer's automated test sets, the evaluator performed a sample of the manual testing to confirm the results and test procedure are as expected.

2.6.2 Independent Penetration Testing

The AVA_VAN.5 assurance class requires the evaluator to conduct a methodical vulnerability analysis based on publicly available source of information and based on structured examination of the evidence while performing previous evaluation activities (ASE, ADV, AGD, ATE).

In the AVA_VAN.5 refinement defined in *[EN419221-5]* is required that, the TOE hardware is tested as described in section 7.7.2 Physical security general requirements and section 7.7.3 Physical security requirements for each physical security embodiment in *[ISO 19790]* for Security Level 3. These tests were performed by the developer and verified by the evaluator in their ATE analysis.

Given that restriction in the [PP] on physical attack, the vulnerability analysis focused on logical attacks. The methodology for which involved the following five steps:

- Step 1: The first step of this type of vulnerability analysis is the identification of areas of concern. The areas of concern are identified by the evaluator using the generic weaknesses enumeration database, an open source publicly maintained dictionary of SW weaknesses.
- Step 2: collecting possible vulnerabilities from the design assessment by asking security questions inspired by generic weaknesses separately for all security implementations of the TOE.
- Step 3: collecting possible vulnerabilities from applicable attack lists and public vulnerability search.
- Step 4: These security relevant questions are then translated into TOE-specific possible vulnerabilities.
- Step 5: the evaluator argued whether a possible vulnerability is removed or sufficiently mitigated by the TOE implementation/environment/functional testing evidence. If yes, the possible vulnerability is considered as solved, otherwise it is uniquely labelled as potential vulnerability. Potential vulnerabilities are then addressed in the context of further assessment, penetration tests and/or further code review. In the baseline evaluation, the analysis led to execution of three penetration tests.

The vulnerability analysis was refreshed during this re-evaluation in light of the changes made to the TOE and new developments in attack methodologies. No additional penetration tests were deemed necessary.

2.6.3 Test Configuration

The testing was performed on the nShield Solo XC F2 (PCIe board) installed in a COTS server. This is representative for all TOE variants. The evaluator performed testing using an earlier release of the firmware (12.60.13). The changes between 12.60.13 and the TOE version 12.60.15 were analysed and the evaluator confirmed that the test results obtained were equally applicable for the 12.60.15 release.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

2.7 Re-used evaluation results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE. This was supported by further (remote) site audits performed during the conduct of this re-evaluation

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number nShield Solo XC Hardware Security Module v12.60.15, with the firmware and hardware components are detailed in section Identification of Target of Evaluation above.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the nShield Solo XC Hardware Security Module v12.60.15, to be **CC Part 2 extended, CC Part 3 refined**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5 and ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[EN419221-5]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

The users are advised to carefully verify the hardware version as described in the "Standalone Solo XC configuration" section of *nShield Solo XC Common Criteria Evaluated Configuration Guide*, including a check that the serial number is of the form 46-Xnnnnn A.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

3 Security Target

The nShield Solo XC HSM Security Target, version 1.1, dated Tuesday, March 09, 2021 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report “nShield Solo XC Hardware Security Module v12.60.15” – EAL4+, 20-RPT-1247, v2.0, 10 March 2021.

[ISO 19790] ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules.

[JIL-AAPHD] Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020.

[JIL-AMHD] Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution).

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[EN419221-5] EN 419 221-5:2018, Protection Profiles for TSP Cryptographic Modules – Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020.

[ST] nShield Solo XC HSM Security Target, version 1.1, dated Tuesday, March 09, 2021.

(This is the end of this report).