Certificate Report

Version 1.0

27 June 2022

CSA_CC_21008

For

nShield Solo XC Hardware Security Module Version 12.60.15

From

Entrust

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorising Nation under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	27 June 2022	For release

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the nShield Solo XC Hardware Security Module (HSM) v12.60.15 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

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 for an extensive range of commercial and custom-built applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenisation, SSL/TLS, and code signing.

The nShield Solo XC HSM can also be embedded inside the nShield Connect XC, a 1U server chassis network-attached appliance delivering cryptographic services as a shared network resource for distributed applications and virtual machines.

The TOE comprises the following:

Type	Name	Identifier
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)
Firmware	Solo XC firmware image	v12.60.15
Documentation	nShield Solo XC Common Criteria Evaluated Configuration Guide	v1.1.1

Table 1: TOE Deliverables Overview

The evaluation of the TOE has been carried out by SGS Brightsight, an approved CC test laboratory at the assurance level CC EAL 4, augmented by ALC_FLR.2 & AVA_VAN.5 and completed on 27 June 2022.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
Cryptographic functions, including digital signature, encryption/decryption, key agreement, message digest, message authentication, key generation
Random Number Generation compliant with [AIS31] and NIST [SP 800-90A]
Secure key management
Secure logging
Physical tamper resistance meeting [ISO 19790] Level 3

Table 2: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1].

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 CERTIFICATION 8

1.1 PROCEDURE 8
1.2 RECOGNITION AGREEMENTS 8

2 VALIDITY OF THE CERTIFICATION RESULT 9

3 IDENTIFICATION 10

4 SECURITY POLICY 12

5 ASSUMPTIONS AND SCOPE OF EVALUATION 12

5.1 ASSUMPTIONS 12
5.2 CLARIFICATION OF SCOPE 14
5.3 EVALUATED CONFIGURATION 15
5.4 NON-EVALUATED FUNCTIONALITIES 15
5.5 NON-TOE COMPONENTS 15

6 ARCHITECTURE DESIGN INFORMATION 16

7 DOCUMENTATION 16

8 IT PRODUCT TESTING 16

8.1 DEVELOPER TESTING (ATE_FUN) 16
8.1.1 Test Approach and Depth 16
8.1.2 Test Configuration 17
8.1.3 Test Results 17
8.2 EVALUATOR TESTING (ATE_IND) 18
8.2.1 Test Approach and Depth 18
8.2.2 Test Configuration 18
The same test configuration as described in section 8.1.2. 18
8.2.3 Test Results 18
8.3 PENETRATION TESTING (AVA_VAN) 18
8.3.1 Test Approach and Depth 18

9 RESULTS OF THE EVALUATION 19

10 OBLIGATIONS AND RECOMMENDATIONS FOR THE USAGE OF THE TOE 20

11 ACRONYMS 21

12 BIBLIOGRAPHY 22

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is covered partially by the CCRA for the components up to EAL2.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **26 June 2027**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e., re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: nShield Solo XC Hardware Security Module v12.60.15.

The following table identifies the TOE deliverables.

Type	Name	Identifier	Form Factor	Delivery Mode
Hardware	nShield Solo XC F2	nC3025E-000 rev 06	PCIe board	Courier
	nShield Solo XC F3	nC4035E-000 rev 06	PCIe board	Courier
	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)	PCIe board embedded in 1U nShield Connect XC appliance	Courier
Firmware	Solo XC firmware image	v12.60.15	.nff binary image file in ISO image or DVD	Courier or Web download
Documentation	nShield Solo XC Common Criteria Evaluated Configuration Guide	v1.1.1	pdf file	Courier or Web download

Table 3: TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE are described in Chapter 2 of the guidance document [9].

Additional identification information relevant to this Certification procedure as follows:

TOE	nShield Solo XC Hardware Security Module v12.60.15
Security Target	nShield Solo XC HSM Security Target, Version 1.1.1, 11 June 2021
Developer	Entrust
Sponsor	Entrust
Evaluation Facility	SGS Brightsight
Completion Date of Evaluation	27 June 2022
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_21008
Certificate Validity	5 years from date of issuance

Table 4: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Cryptographic Support
- Identification and Authentication
- User Data Protection
- Trusted Path/Channels
- Protection of the TSF
- Security Management
- Security Audit

Specific details concerning the above mentioned security policy can be found in Chapter 6 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Assumptions	Description
A.ExternalData Protection of data outside TOE control	Where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities must provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment. In particular, any backups of the TOE and its data are maintained in a way that ensures appropriate controls over making backups, storing backup data, and using backup data to restore an operational TOE. The number of sets of backup data does not exceed the minimum needed to ensure continuity of the TSP service. The ability to restore a TOE to an operational state from backup data requires at least dual person control (i.e. the participation and approval of more than one authenticated administrator).

A.Env Protected operating environment	The TOE operates in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE software and hardware environment (including client applications) is installed maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment.
A.DataContext Appropriate use of TOE functions	Any client application using the cryptographic functions of the TOE will ensure that the correct data are supplied in a secure manner (including any relevant requirements for authenticity, integrity and confidentiality). For example, when creating a digital signature over a DTBS the client application will ensure that the correct (authentic, unmodified) DTBS/R is supplied to the TOE, and will correctly and securely manage the signature received from the TOE; and when certifying a public key the client application will ensure that necessary checks are made to prove possession of the corresponding private key. The client application may make use of appropriate secure channels provided by the TOE to support these security requirements. Where required by the risks in the operational environment a suitable entity (possibly the client application) performs a check of the signature returned from the TOE, to confirm that it relates to the correct DTBS. Client applications are also responsible for any required logging of the uses made of the TOE services, such as signing (or sealing) events. Similar requirements apply in local use cases where no client application need be involved, but in which the TOE and its user data (such as keys used for signatures) need to be configured in ways that will support the need for security requirements such as sole control of signing keys. Appropriate procedures are defined for the initial creation of data and continuing operation of the TOE according to the specific risks applicable to the deployment environment and the ways in which the TOE is used.
A.UAuth Authentication of application users	Any client application using the cryptographic services of the TOE will correctly and securely gather identification and authentication/authorisation data from its users and securely transfer it to the TOE (protecting the confidentiality of the

	authentication/authorisation data as required) when required to authorise the use of TOE assets and services.
A.AuditSupport Audit data review	The audit trail generated by the TOE will be collected, maintained and reviewed by a System Auditor according to a defined audit procedure for the TSP.
A.AppSupport Application security support	Procedures to ensure the ongoing security of client applications and their data will be defined and followed in the environment, and reflected in use of the appropriate TOE cryptographic functions and parameters, and appropriate management and administration actions on the TOE. This includes, for example, any relevant policies on algorithms, key generation methods, key lengths, key access, key import/export, key usage limitations, key activation, cryptoperiods and key renewal, and key/certificate revocation.

Table 5: Assumptions

Details can be found in section 3.5 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

5.3 Evaluated Configuration

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

Figure 1: nShield Solo XC

Figure 2: nShield Connect XC HSM

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE does not require additional components for its operation.

6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:

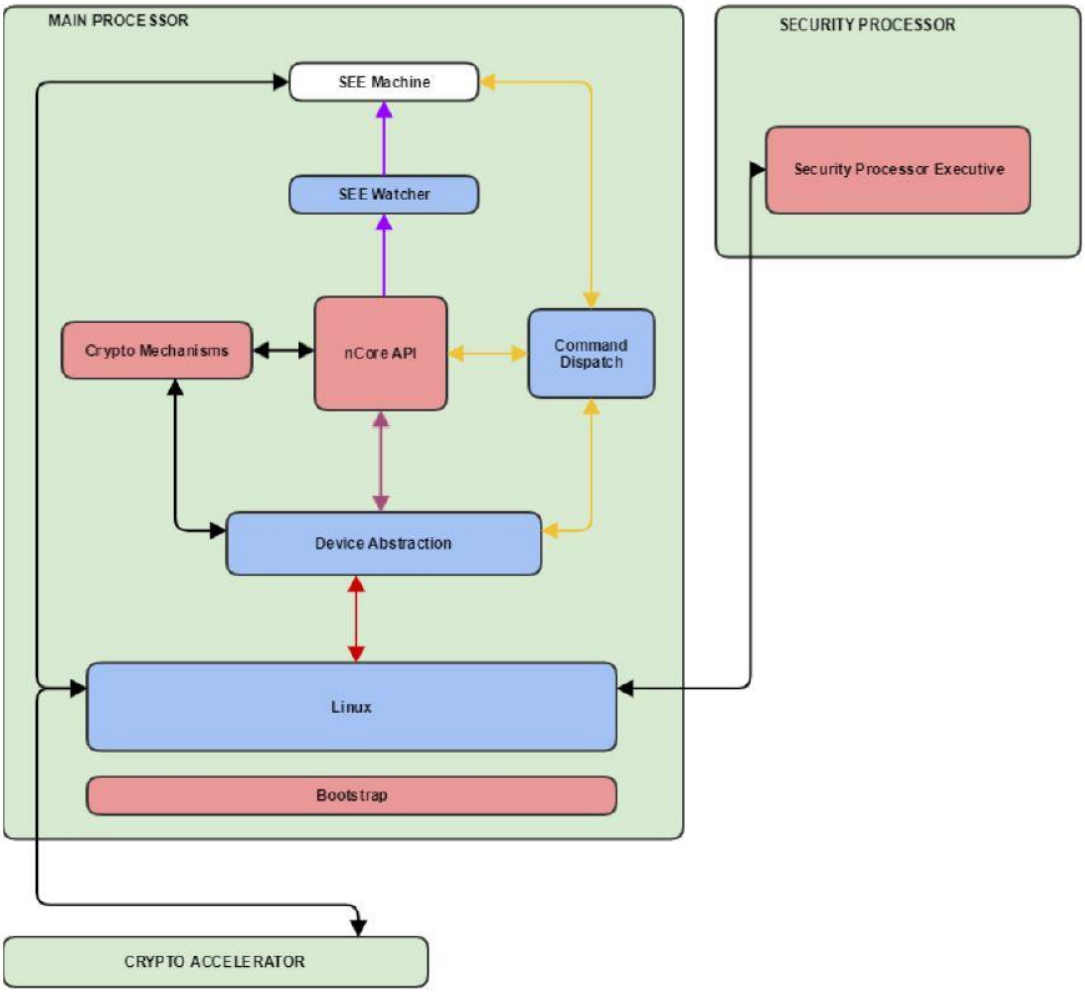

Figure 3: Logical Architecture of the TOE

7 Documentation

The evaluated documentation as listed in Table 3: TOE Deliverables is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

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 the CAVS verification tool and the OpenSSL implementation. Additionally, the developer implemented a set of manual test to demonstrate the correct behaviour of the all the TSFIs

For all the tests, log files are 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.

8.1.2 Test Configuration

The network diagram describes the base setup used for both developer's and evaluator's testing.

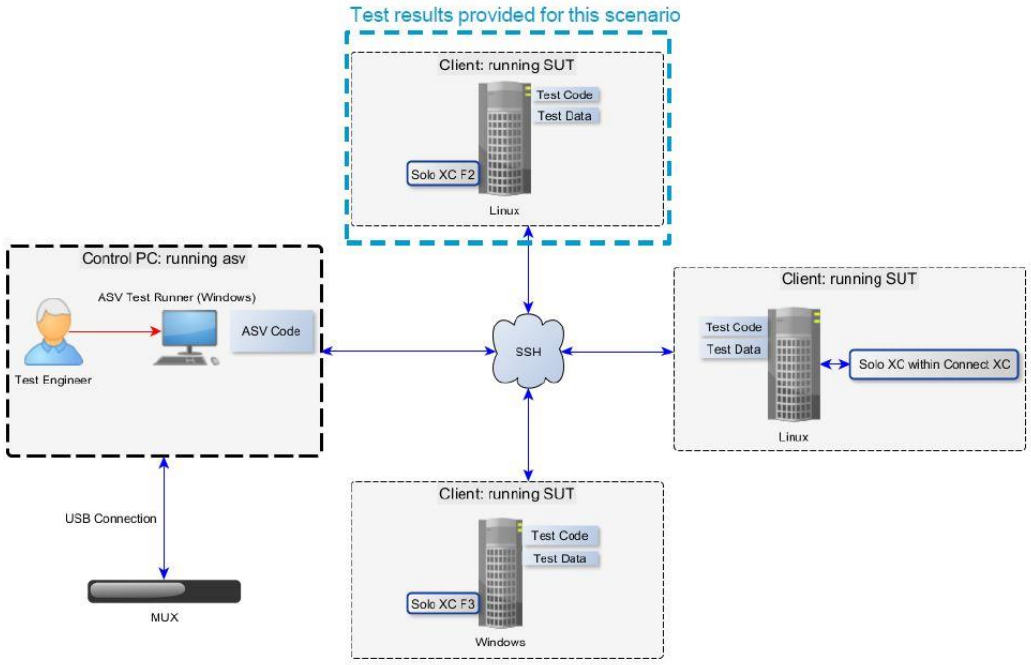

Figure 4: Developer's Test Setup

The developer implemented a proprietary test environment to allow interface testing of the TOE. The automatic test are invoked via the ASV Test Runners, which is executed on the CONTROL PC and implemented in C#. The actual Test Code is executed on CLIENT TEST MACHINE and mostly implemented in Python. The test results are collected and verified by the Test Code and sent back to the ASV Test Runners. The ASV Test Runners then composes human readable test report. The MUX card reader consists of ten card readers and cards, which simulates a manual card swap.

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1], with the exception of the Clear Button and the Mode Switch which were then verified as part of ATE_IND.

All actual test results from all tested environments are identical to the expected test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluator analysed the developer's test coverage, test plans and procedures, expected and actual test results.

The evaluator repeated all the developers tests 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.

In addition to the repeated automated testing, the evaluator performed a sample of the manual testing to confirm their results and test procedure is as expected.

8.2.2 Test Configuration

The same test configuration as described in section 8.1.2.

8.2.3 Test Results

The evaluator concluded that the developer tests and the evaluator independent tests fully tested the TOE functionalities and security behaviours. The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

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).

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.5) treating the resistance of the TOE to an attack with the High attack potential.

Test ID	Description
PEN_TEST_MONTG_REDUCTION_TIMING	Gain assurance whether an attacker can distinguish the presence or absence of modular reductions within the RSA-CRT private operation through its global execution time.
PEN_TEST_ENUMERATE_NVRAM	In this test is verified that no confidential data can be downloaded from the NVRAM in one of the

	different phases of the TOE (e.g. creating a security world, when the administrator is logged in, key user is created). The test should show that no confidential data is loaded on the TOE.
PEN_TEST_MANIPULATE_SW_ON_NVRAM	In this test is verified that the software package on the TOE, which is loaded in NVRAM, cannot be manipulated.

Table 6: Penetration Test Cases

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 augmented by ALC_FLR.2 and AVA_VAN.5 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 3: TOE Deliverables contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

The users must carefully verify the HW version as described in [9], including a check that the serial number is of the form 46-Xnnnnn A.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Entrust, “nShield Solo XC HSM Security Target Version 1.1.1,” 2021.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] Entrust, “nShield Solo XC Common Criteria Evaluated Configuration Guide v1.1.1”.

[10] EN 419 221-5:2018 version 1.0, “Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trusted Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01,” 18 May 2020.

[11] SGS Brightsight, “Evaluation Technical Report "nShield Solo XC Hardware Security Module v12.60.15" - EAL4+,” 2022.

----------End of Report ----------