



# Certificate Report

## Version 1.0

## 24 September 2024

## CSA_CC_23004

## For

## nShield5s Hardware Security Module
## Version 13.5.1

## From

## Entrust

This page is left blank intentionally

# Foreword

Singapore is a Common Criteria Certificate Authorizing 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 | 24 September 2024 | Released |

**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 nShield5s Hardware Security Module (HSM) v13.5.1 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The TOE is a general purpose Cryptographic Module (HSM) 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 Client Applications including public key infrastructures (PKIs), identity management systems, application level encryption and tokenization, and code signing.

The TOE comprises of the following components:

| Type | Name | Identifier |
|---|---|---|
| Hardware | nShield5s<br>Form Factor - PCIe Board | NC5536E |
| | nShield5s<br>Form Factor – PCIe Board<br>embedded in nShield5c chassis | NC5536N |
| Firmware | nShield5s Primary | v13.5.1 |
| | nShield5s Recovery | v13.5.0 |
| | nShield5s Bootloader | v1.4.1 |

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

| Name | Version | Method of Delivery |
|---|---|---|
| nShield5 Common Criteria Evaluated Configuration Guide (PDF) | v6.0 | Web Download |

Table 2 - List of guidance documents

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 with AVA_VAN.5 (Advanced Methodical Vulnerability Analysis) and completed on 30 April 2024.

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 of audit records |
| Physical tamper resistance meeting [ISO 19790] Level 3 |

Table 3: 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

## 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 partially covered by the CCRA.

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 **23 September 2029**[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 (https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list) for the up-to-date status regarding the certificate's validity.

# 3 Identification

The Target of Evaluation (TOE) is: nShield5s Hardware Security Module (HSM) v13.5.1.

The following table identifies the TOE deliverables.
The TOE comprises of the following components:

| Type | Name | Identifier |
|---|---|---|
| Hardware | nShield5s<br>Form Factor - PCIe Board | NC5536E |
| | nShield5s<br>Form Factor – PCIe Board embedded in nShield5c chassis | NC5536N |
| Firmware | nShield5s Primary | v13.5.1 |
| | nShield5s Recovery | v13.5.0 |
| | nShield5s Bootloader | v1.4.1 |
| Documentation | nShield5 Common Criteria Evaluated Configuration Guide | v6.0 |

Table 4 - TOE Deliverables

Additional identification information relevant to this Certification procedure as follows:

| | |
|---|---|
| TOE | nShield5s Hardware Security Module v13.5.1 |
| Security Target | nShield5s HSM Security Target v12 |
| Developer | Entrust |
| Sponsor | Entrust |
| Evaluation Facility | SGS Brightsight |
| Completion Date of Evaluation | 30 April 2024 |
| Certification Body | Cyber Security Agency of Singapore (CSA) |
| Certificate ID | CSA_CC_23004 |
| Certificate | 5 years from date of issuance |

| | |
|---|---|
| Validity | |

Table 5: 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/Channel
- 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:

| Environmental Assumptions | Description |
|---|---|
| OE.ExternalData<br><br>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 shall provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment. This includes protection of data that is exported from, or imported to, the TOE (such as audit data and encrypted keys).<br>In particular, any backups of the TOE and its data shall be 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 shall 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 shall require at least dual person control (i.e. the participation and approval of more than one authenticated administrator). |

| | |
|---|---|
| OE.Env<br><br>Protected operating environment | The TOE shall operate in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE software and hardware environment (including client applications) shall be installed and maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment, including (where applicable):<br>• Protection against loss or theft of the TOE or any of its externally stored assets<br>• Inspections to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the TOE, or parts of the hardware appliance)<br>• Protection against the possibility of attacks based on emanations from the TOE (e.g. electromagnetic emanations) according to risks assessed for the operating environment<br>• Protection against unauthorised software and configuration changes on the TOE and the hardware appliance<br>• Protection to an equivalent level of all instances of the TOE holding the same assets (e.g. where a key is present as a backup in more than one instance of the TOE). |
| OE.DataContext<br><br>Appropriate use of TOE functions | Any client application using the cryptographic functions of the TOE shall 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 shall ensure that the correct (authentic, unmodified) DTBS/R is supplied to the TOE, and shall correctly and securely manage the signature received from the TOE; and when certifying a public key the client application shall 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 suppose these security requirements. Where required by the risks in the operational environment a suitable entity (possibly the client application) shall perform a check of the signature returned from the TOE, to confirm that it relates to the correct DTBS.<br><br>Client applications shall be responsible for any required logging of the uses made of the TOE service, such as signing (or sealing) events. |

| | |
|---|---|
| | Similar requirements shall 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.<br><br>Appropriate procedures shall be defined for the initial creation of data and continuing operating of the TOE according to the specific risks applicable to the deployment environment and the ways in which the TOE is used. |
| OE.Uauth<br><br>Authentication of application users | Any client application using the cryptographic services of the TOE shall 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. |
| OE.Audit<br><br>Support 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.<br><br>Application Note: As noted for P.Audit, the TOE is assumed to exist as part of a larger system and the System Auditor is a role within this larger system. |
| OE.AppSupport<br><br>Application security support | Procedures to ensure the ongoing security of client applications and their data shall 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 length, key access, key import/export, key usages limitations, key activation, cryptoperiods and key renewal, and key/certificate revocation. |

Table 6: Environmental Assumptions

Details can be found in section 4.2 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].

Users are reminded to set up the TOE as per guidance documents (FIPS mode) to correctly deploy and use the TOE in the evaluated configuration.

## 5.3 Evaluated Configuration

The TOE is a general-purpose Cryptographic Module (HSM) 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 Client Applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenization, and code signing.


*Figure 1 - nShield5s PCIe Board*


*Figure 2 - nShield5c Appliance*

## 5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 0.

## 5.5 Non-TOE Components

The TOE following hardware and software, which is not part of the evaluation scope is required by the TOE:

- nShield5c network appliance or host PC/Server, depending on the configuration

- Host side software, including drivers, Hardserver, and high level APIs which are provided by Entrust
- Set of smartcards, TVD and module warrant certificate, provided by Entrust for card-based authentication
- Syslog server for long term storage of audit logs

# 6 Architecture Design Information

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

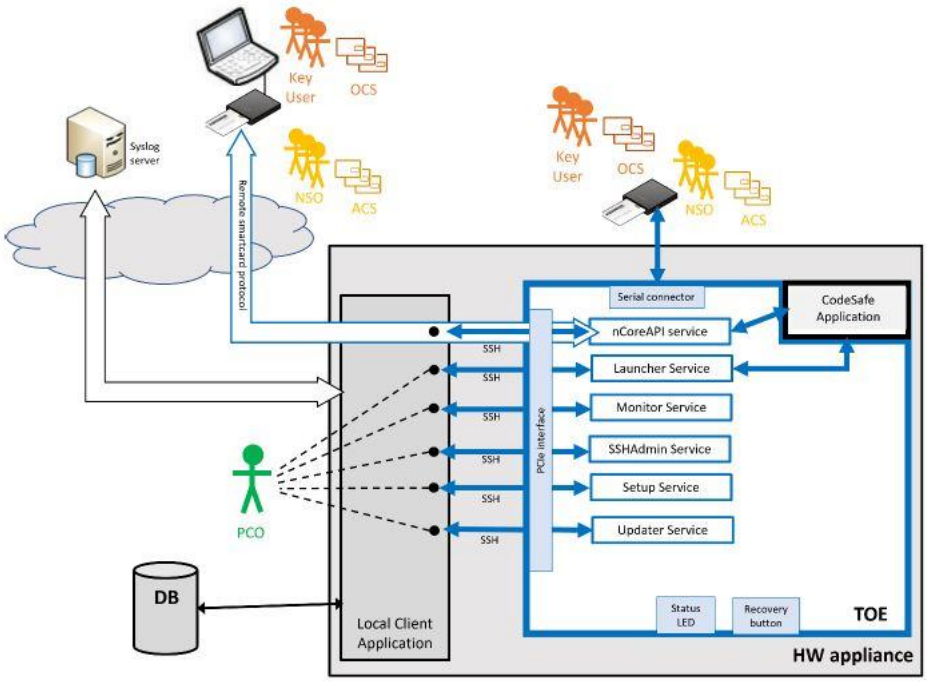


Figure 3 - Logical Architecture of the TOE (From [ST])

The TOE has the following features:

- Cryptographic functions, including digital signature, encryption, decryption, key agreement, message digest, message authentication, key generation
- Secure logging of audit records
- Physical tamper resistance meeting ISO-19790 Level 3

The TOE can be used as a general Cryptographic Module in a wide range of use cases, including but not limited to Trust Service Providers, for example with EN 419 241-2 to provide a QSCD for remote Server Signing.

# 7 Documentation

The evaluated documentation as listed in **Error! Reference source not found.** 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

The developer performed functional testing covering all TSFIs and module-to-

module interactions. Several proprietary automated test suites were used, along with cryptographic tests suites such as known-answer tests and physical hardware tests to fulfil FPT_PHP.1 and FPT_PHP.3 requirements.

### 8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [10].

### 8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

## 8.2 Evaluator Testing (ATE_IND)

### 8.2.1 Test Approach and Depth

The automated functional test cases implemented in the ASV Test Environment were repeated by the evaluator.

The evaluator's strategy for devising independent tests was based on the following:

- If a SFR is not fully covered by the developer's tests or a specific case was not tested (e.g. positive test was performed but not a negative test)
- Important features that other countermeasures are built upon (e.g. blobbing) or security primitives that provide support to other security features (e.g. random numbers)
- Specific corner cases not tested or fully clear

### 8.2.2 Test Configuration

A detailed test description was provided in the ATE document. The evaluator used the developer's test environment at the developer's premises to perform independent testing. Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

### 8.2.3 Test Results

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).

Given the restrictions imposed by the PP (which prevents any physical attack

and any side channel attack that requires physical proximity to the TOE), the evaluator focused on vulnerabilities related to design/architectural flaws that would lead intended users to abuse the TOE. For this reason, the evaluator needed to find a methodical approach to scout the TOE implementation searching for such design/architectural flaws.

The evaluator's strategy for performing vulnerability analysis was based on the following:

1. Identification of areas of concern using open source publicly maintained weakness enumeration database. Areas of concerns includes Accessibility, Cryptography, Secure Channel etc.
2. Collecting possible vulnerabilities from the design assessment by asking security questions inspired by general weaknesses separately for all security implementations of the TOE
3. Collecting possible vulnerabilities from applicable attack lists and public vulnerability search
4. Translating security relevant questions into TOE-specific possible vulnerabilities
5. The evaluator then justifies 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 and then addressed in the context of penetration tests and/or further code review.

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.

| Penetration Test | Description |
|---|---|
| PEN_TEST_ENUMERATE_NVRAM | Verifying that no confidential data can be downloaded from the NVRAM in one of the different phases of the TOE (i.e. creating a security world, when the administrator is logged in, key user is created). |
| PEN_TEST_MANIPULATE_SW_ON_NVRAM | Verifying that the software package on the TOE, which is loaded in NVRAM, cannot be manipulated |

Table 7 - Penetration Test Case

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 2 - List of guidance documents 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.

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

No additional recommendation was provided by the evaluators.

# 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, “nShield5s HSM Security Target Version 12,” 24 April 2024.

[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, “nShield5 Common Criteria Evaluated Configuration Guide Version 19,” 9 October 2023.

[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] Brightsight B.V., “Evaluation Technical Report 24-RPT-434 nShield5s Hardware Security Module v13.5.1 - EAL4+,” 30 April 2024.


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