Certification Report

nShield5s Hardware Security Module v13.5.1

Sponsor and developer: ***Entrust***
One Station Square,
Cambridge, CB1 2GA,
United Kingdom

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-2200057-01-CR**
Report version:	**1**
Project number:	NSCIB-**2200057-01**
Author(s):	**Wim Ton**
Date:	**11 April 2024**
Number of pages:	**13**
Number of appendices:	**0**

CONTENTS

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, TrustCB 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 TrustCB 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 TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence 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, TrustCB 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, 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 (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the nShield5s Hardware Security Module v13.5.1. The developer of the nShield5s Hardware Security Module v13.5.1 is Entrust located in Cambridge, United Kingdom and they also act as the sponsor of the evaluation and certification. 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 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 has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 10 April 2024 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the nShield5s Hardware Security Module v13.5.1, 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 nShield5s Hardware Security Module v13.5.1 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 provide 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 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB 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. Note that the certification results apply only to the specific version of the product as evaluated.

The TOE is stated as a Qualified Signature Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the nShield5s Hardware Security Module v13.5.1 from Entrust located in Cambridge, United Kingdom.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	nShield5s	NC5536E, PCB assembly part number PCA10005-01 revision 03
	nShield5c	NC5536N, PCB assembly part number PCA10005-01 revision 03 in a NH2096 server
Software	Bootloader	1.4.0
	nShield5s recovery image	13.5.0
	nShield5s firmware image	13.5.1

The TOE can be a PCI card for integration by the user (nShield5s), or the same card is delivered pre-integrated in a server (nShield5c).

To ensure secure usage, a set of guidance documents is provided, together with the nShield5s Hardware Security Module v13.5.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

Hardware Security Module

The following cryptographic primitives are supported and included within the TSF:

The TOE has the following features:

- Cryptographic functions, including digital signature, encryption/decryption, key agreement, message digest, message authentication, key generation[2].
  - AES in ECB, CBC, GCM, CMAC, KW, and KWP mode with key lengths of 128, 192, and 256 bits
  - ECDSA, ECDH, and ECQMV with NIST and Brainpool curves
  - RSA with OEAP, RSASSA-PKCS-v1_5, and RSASSA-PSS padding and modulus lengths of 2048, 3072, and 4096 bits (plus 1024 bits only for signature verification)
  - DSA with modulus lengths of 2048 and 3072 bits (plus 1024 bits only for signature verification)
  - Diffie Helman with modulus lengths from 2048 to 8192 bits
  - KDF functions
  - SHA-1, SHA-2, and SHA-3 hashes
  - HMAC with SHA-1 and SHA-2 with a MAC length > 112 bits
- Random Number Generation compliant with AIS-31 and NIST SP 800-90A,
- Secure key management,

[2] See *[ST]* chapter 1.3.3.1 for the details

- Secure logging of audit records to an external server,
- Physical tamper resistance meeting ISO-19790 Level 3.
- Signed firmware updates.

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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

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 in which it is contained ("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.

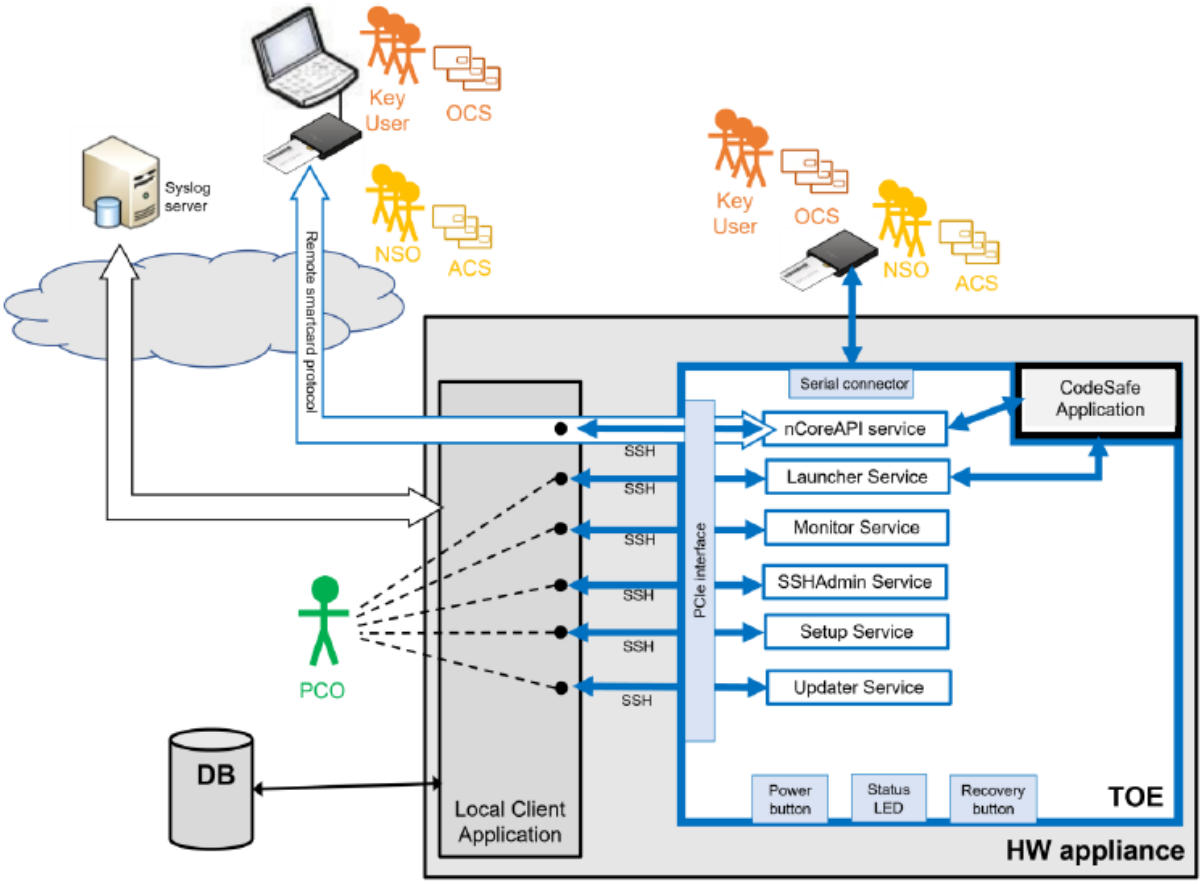
Any threats violating these objectives for the environment are not considered.

2.4 Architectural Information

The logical boundary of the TOE (indicated in blue in the picture below) comprises the firmware located inside the PCIe board, with the exception of embedded CodeSafe applications and is schematically represented by the following logical components.

The picture below includes also non-TOE components (such as Local Client Application, HW appliance, external databases, syslog server and smartcard readers), which are functionally required by the TOE, but do not enforce the security requirements listed in the Security Target *[ST]*.

With nShield HSMs, keys never leave the physical HSM in an unprotected form.



The TOE stores all user data externally in the “Security World”, secured with a user specific key. This key can be retrieved from a quorum of smartcards in the “Operator Card Set”.

2.5 Documentation

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

Identifier	Version
nShield5 Common Criteria Evaluated Configuration Guide	V26

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 evaluator repeated all automated developer tests and confirmed that these all pass.

The evaluator created additional test cases test to confirm verification of the version of the TOE, to supplement coverage of SFRs, and to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

For the collection of possible vulnerabilities, a methodical approach is taken which consists of:

- Possible vulnerabilities found during the Design Assessment

- Using applicable attack lists
- Public vulnerability search

The total test effort expended by the evaluators was 2 weeks (80 hours). During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

Testing was conducted at the developer site, using the test equipment from the developer.

2.6.4 Test 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 Evaluated Configuration

The TOE is defined uniquely by its name and version number nShield5s Hardware Security Module v13.5.1. Chapter 9.1.1 of the installation guide describes how to read the version number and operational status of the TOE.

2.8 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the development *[STAR-C]* and for the manufacturing *[STAR-P]* [3] sites.

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

Based on the above evaluation results the evaluation lab concluded the nShield5s Hardware Security Module v13.5.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2 and AVA_VAN.5**.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]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" 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 concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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. For the evolution of attack methods and techniques to be covered, the

[3] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

customer 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 algorithms, protocols and implementations[4]:

- The algorithms in section 2.2 with shorter key-lengths, custom curves, and other modes.
- DES and 3DES
- Aria
- RC4
- Cast-256
- Camellia
- KTS-OAEP-basic
- KCDSA
- SEED
- X25519 key exchange
- Ed25519 public-key signature
- ElGamal
- ECKA-EG key agreement
- ECIES encryption/wrapping and decryption/unwrapping
- MD5, RIPEMD-160 and Tiger hashes
- EMV ARQC MAC
- 3GPP TUAK and Milenage

, which are out of scope as there are no security claims relating to these.

[4] See chapter 1.3.3.2 of the *[ST]*

3 Security Target

The nShield5 HSM Security Target, Version 112, 8 March 2024 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

ACL	Access Control List
AES	Advanced Encryption Standard
ACS	Administrator Card Set - a set of smart cards used to control access to Administration functions.
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DCAP	Dutch Conformity Assessment Process
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois Counter Mode
IC	Integrated Circuit
JIL	Joint Interpretation Library
KDF	Key Derivation Function
KW	Key Wrap
LAN	Local Area Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NSO	nShield Security Officer
OCS	Operator Card Set- a set of smart cards used to control access to user functions.
PCO	Platform Crypto Officer, the TOE administrator
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key
QSCD	Qualified Signature/Seal Creation Device
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SCD	Signature Creation Device

SDK	System Development Kit
SHA	Secure Hash Algorithm
SM	Secure Messaging
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TRNG	True Random Number Generator
VLAN	Virtual LAN

5 Bibliography

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

[ASS-EIDAS]	Assessment reporting sheet eIDAS, 24-RPT-144, Version 2.0,14 February 2024
[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
[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
[ETR]	Evaluation Technical Report | nShield5 Hardware Security Module v13.5.1 – EAL4+, 23-RPT-699, Version 7.0,10 April 2024
[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[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 2.6, 02 August 2022
[ST]	nShield5 HSM Security Target, Version 112, 8 March 2024
[STAR-C]	Site Technical Audit Report Cambridge, 24-RPT-118, Version 3.0, 10 April 2024
[STAR-P]	Site Technical Audit Report Plexus, 24-RPT-117, Version 3.0, 10 April 2024

(This is the end of this report.)