Certification Report

NXP SmartePP on P71, version 03 00 00 10

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Troplowitzstrasse 20
22529 Hamburg
Germany

Evaluation facility: ***Riscure B.V***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-0108259-CR**
Report version:	**1**
Project number:	**0108259**
Author(s):	**Jordi Mujal**
Date:	**16 April 2021**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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

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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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 NXP SmartePP on P71, version 03 00 00 10. The developer of the NXP SmartePP on P71, version 03 00 00 10 is NXP Semiconductors Germany GmbH located in Hamburg, Germany 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 the NXP Smart ePP on P71 Secure Element. It implements a native operating system and an application compliant with ICAO specifications referenced in the *[ST]*. The TOE supports the advanced security methods Basic Access Control (BAC) and Active Authentication, and this certification applies to the BAC configuration with or without Active Authentication. The TOE is a composite TOE based upon the underlying P71 platform with its Crypto Library and Software Library.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 16 April 2021 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 NXP SmartePP on P71, version 03 00 00 10, 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 NXP SmartePP on P71, version 03 00 00 10 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_DVS.2 (Sufficiency of security measures) and ALC_FLR.1 (Basic flaw remediation).

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 NXP SmartePP on P71, version 03 00 00 10 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP Secure Smart Card Controller N7121	B1
Software Libraries	IC Dedicated Software	9.2.3.0
Software Libraries	IC Dedicated Crypto Library	0.7.6
Software	53 6D 61 72 74 65 50 50 -"SmartePP"	03 00 00 10

To ensure secure usage a set of guidance documents is provided together with the NXP SmartePP on P71, version 03 00 00 10. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.3.5.

2.2 Security Policy

The Target of Evaluation (TOE) is the integrated circuit chip of the machine readable travel document (MRTD chip), loaded with a the native Card Operating System, SmartePP, programmed with the Logical Data Structure (LDS) providing Basic Access Control (BAC) and optionally Active Authentication. TOE functionality is according to ICAO Documents referenced in the *[ST]* and the set of Security Functional Requirements defined in the *[ST]* and implemented by the TOE.

The TOE features include

- Authentication mechanisms in accordance to the ICAO specification:
  - Basic access control (BAC)
  - Active authentication (AA)
- Access control to allow retrieval of less sensitive data.

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 the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalized must perform proper and safe personalization according to the guidance and referred ICAO guidelines.

The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

2.4 Architectural Information

The TOE is a native OS called Smart ePP running on top of an already evaluated base TOE subsystem comprising:

- the circuitry of the MRTD's chip, assessed as part of the base TOE subsystem evaluation
- the IC Dedicated Software and Crypto Library, assessed as part of the base TOE subsystem evaluation
- the IC Embedded Software (smart ePP)
- a personalised filesystem, created in accordance with the guidance

2.5 Documentation

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

Identifier	Version
SmartePP User manual and administrator guide	1.4
SmartePP ICAO Personalization Guide	1.4

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 module level. All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

The test results of the underlying base TOE are extendable to composite evaluations, as the base TOE is used according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The vulnerability analysis was performed based on the structure of the attack methods defined by JHAS *[JIL-AM]* and *[JIL-AAPS]*. For each attack method, we describe the objective of the attack and how the attack method applies to the TOE. The following was considered for each attack method:

- The design and implementation of the features relevant for the attack method
- Specific attack techniques from the evaluator's attack repository
- Implemented countermeasures
- User guidance and ETRfc from the underlying platform *[HW-ETRfc]*.

Based on these items, it was determined whether an attack method was applicable to the TOE and should be tested during the penetration testing phase.

The total test effort expended by the evaluators was 6 weeks. During that test campaign 100% of the total time was spent on Perturbation attacks.

2.6.3 Test Configuration

The identity and configuration of the hardware and software was verified in accordance with the procedures and information presented in *[ST]* and the TOE guidance presented in section 2.5.

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

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 6 site certificates.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP SmartePP on P71, version 03 00 00 10. The guidance documents describe how to verify the TOE and configure it.

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 NXP SmartePP on P71, version 03 00 00 10, to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims strict conformance to the Protection Profile *[PP].*

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.

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 Security Target NXP SmartePP on P71 - BAC, v1.5, 02 March 2021 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

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

BAC	Basic Access Control
EAC	Extended Access Control
eMRTD	electronic MRTD
ICAO	International Civil Aviation Organization
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
TOE	Target of Evaluation

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 for NXP Smart ePP on P71 - ICAO EAC with SAC/PACE and NXP Smart ePP on P71 - BAC 03 00 00 10, 20190534-D3, v1.6, 14 April 2021.
[HW-CERT]	Certification report - BSI-DSZ-CC-1136-2021 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) from NXP Semiconductors Germany GmbH,10 February 2021.
[HW-ETRfC]	Evaluation Technical Report for composite evaluation – NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2), v3, 05 February 2021.
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020.
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution).
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Protection Profile – Machine Readable Travel Document with "ICAO Application" and Basic Access Control (MRTD-PP), version 1.10, 25th March 2009, registered under the reference BSI-CC-PP-0055-2009.
[ST]	Security Target NXP SmartePP on P71 - BAC, v1.5, 02 March 2021.
[ST-lite]	Security Target Lite NXP SmartePP on P71 - BAC, v1.3, 02 March 2021.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).