Certification Report

NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE

Sponsor:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Developer:	***cv cryptovision GmbH*** **Munscheidstr. 14** **45886 Gelsenkirchen** **Germany**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0229285-CR**
Report version:	**1**
Project number:	**0229285**
Author(s):	**Jordi Mujal**
Date:	**18 December 2020**
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

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 NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE. The developer of the NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE is cv cryptovision GmbH located in Gelsenkirchen, Germany. The sponsor of the evaluation and certification was NXP Semiconductors Germany GmbH located in Hamburg, Germany. 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 consists of an applet and the certified Java Card platform (JCOP 4 on P71) *[PL-CERT]* that can be configured to be used as an eMRTD as specified in *[ST]*. After instantiation and configuration as MRTD-EAC configuration it can be programmed amongst others according to the Logical Data Structure (LDS) and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' and BSI TR-03110 documents referenced in the *[ST]*.

The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE.

The TOE is delivered during the preparation phase after which the initialisation and personalisation are performed.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2020/12/18 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 eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, 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 eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) 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 NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE from cv cryptovision GmbH located in Gelsenkirchen, Germany.

The TOE is comprised of the following main components:

	Name	Version
Hardware	NXP secure Smart Card controller N7121 with IC Dedicated Software and Crypto Library	B1
Software	IC dedicated Test Software	9.2.3
	Boot Software	9.2.3
	Firmware	9.2.3
	FlashLoader OS	1.2.5
	Library Interface	9.2.3
	System Mode OS	13.2.3
	Crypto Library	0.7.6
	IC Embedded Software (for "configuration Banking & Secure ID)	JCOP 4.7 P71 R1.01.4
	NXP eDoc Suite on JCOP4 P71 –cryptovision ePasslet Suite	v3.5 (internal version 0405, 3E5E)

To ensure secure usage a set of guidance documents is provided together with the NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE. 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 1.4.

2.2 Security Policy

The TOE is a Java Card (NXP eDoc Suite v3.5 on JCOP4 - cryptovision ePasslet Suite) configured to provide a contact and contactless integrated circuit chip containing components for a machine readable travel document (MRTD). As MRTD-EAC configuration it can be programmed according to the Logical Data Structure (LDS), additionally providing the Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), Active Authentication (AA) and Chip Authentication (CA) according to the ICAO and BSI TR-03110 documents referenced in the *[ST]*.

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.

The TOE can be ordered in 3 configurations:

- 1 configuration without Biometry.

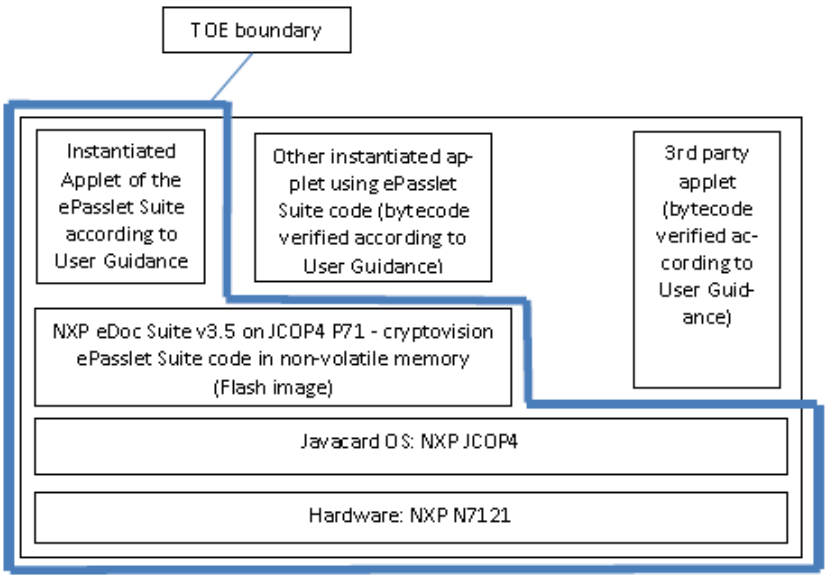
- 2 configurations with Biometry library

It is noted that the Biometry is not claimed in anyway nor specified in the Security Target and considered SFR-Non-interfering.

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 consists of:



- The circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities.
- The platform with the Java Card operation system JCOP4 (NXP JCOP4 P71; please refer to the platform security target *[PL-ST]* for details of this designation), together with the JCOP4 documentation according to *[PL-ST]*.
- NXP eDoc Suite v3.5 on JCOP4 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE.
- The associated guidance documentation: Administrator and User Guidance in PDF format and the platform documentation.

Multiple configurations (and hence support for different applications) can be present at the same time by instantiating multiple applets with their distinct configurations. Such additional functionality is independent of the functionality of the TOE as described in the *[ST]* and the guidance manuals. This is ensured by the isolation properties of the Java Card platform.

2.5 Documentation

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

Name	Version	Date
JCOP 4 P71, User Manual for JCOP 4P71	rev 3.7	2019-05-31
NXP Secure Smart Card controller N7121, Preliminary data sheet	rev 2.0	2018-08-31
NXP eDoc Suite v3.5 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC), Preparation Guidance (AGD_PRE),	version 1.3.1	2020-11-30
NXP eDoc Suite v3.5 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC), Operational Guidance (AGD_OPE),	version 1.2.0	2020-11-24
NXP eDoc Suite v3.5 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications Guidance Manual	version 1.3.1	2020-11-30

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 underlying hardware, crypto-library and Javacard test results are extendable to composite evaluations, as the underlying platform is operated 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 methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack

methods in *[JIL-AP]*. An important source for assurance in this step is the ETR for composition of the underlying platform *[PL-CERT]*.

- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate

The total test effort expended by the evaluators was 2 weeks. During that test campaign 50% of the total time was spent on Perturbation attacks and 50% on logical tests

2.6.3 Test Configuration

It has been tested in pre-personalisation, personalisation and operational life-cycle states with applet instance configurations specified in the Security Target *[ST].*

Functional testing was carried out by witnessing of the developer testing and by repeating some tests by the Laboratory. A combination of standard commercial tools and proprietary developer tools were used. Penetration testing was performed by using the Lab's equipment.

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 is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE. 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 eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.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 *[PP-EAC]* and *[PP-PACE]*.

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 NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE – Security Target, Version 1.2, 2020-12-17 *[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
CA	Chip Authentication
EAC	Extended Access Control
eMRTD	electronic MRTD
ICAO	International Civil Aviation Organization
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
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 “NXP eDoc Suite v3.5 on JCOP4 – cryptovision ePasslet Suite” – EAL5+, 20-RPT-956, v7.0, 2020-12-18.

[JIL-AP] JIL - Application of Attack Potential to Smartcards and Similar Devices Version 3.1, June 2020.

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

[PL-CERT] Certification Report JCOP 4 P71, Report number: NSCIB-CC-180212-CR2, TÜV Rhein-land Nederland B.V., 20 March 2020.

[PL-ST] NXP JCOP 4 P71 Security Target for JCOP 4 P71 / SE050 Rev. 3.7 – 2020-03-17; Evaluation documentation, Final, NSCIB-CC-180212.

[PP-EAC] Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), registered under the reference BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012.

[PP-PACE] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, registered under the reference BSI-CC-PP-0068-V2-MA-01, Version 1.01, 22 July 2014, BSI.

[ST] NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE – Security Target, Version 1.2, 2020-12-17.

[ST-lite] NXP eDoc Suite v3.5 on JCOP4 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE – Security Target Lite, Version 1.2, 2020-12-17.

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).