Certification Report

NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)

Sponsor:	***NXP Semiconductors Germany GmbH*** **Beiersdorfstrasse 12** **D-22529 Hamburg** **Germany**
Developer:	***cv cryptovision GmbH*** **Munscheidstr. 14** **45886 Gelsenkirchen** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2200053-02-CR**
Report version:	**1**
Project number:	**NSCIB-2200053-02**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**03 May 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 NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD). The developer of the NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) is cv cryptovision GmbH located in Gelsenkirchen, Germany and NXP Semiconductors Germany GmbH was 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 Java Card with a set of applets (NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite) configured to provide a secure signature creation device (SSCD) with key generation for the creation of legally binding qualified electronic signatures and qualified electronic seals as defined in the eIDAS regulation. To allow secure access to the signature functionality over the contactless interface, it provides an optional PACE mechanism to build up a secure channel for the verification authentication data (signature password/PIN or data derived from a user's biometric characteristics).

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 09 August 2023. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 3 May 2024 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a "recertification with major changes".

The major change is an additional configuration compared to the set of configuration that has been certified under NSCIB-2200053-01. This configuration, referred to as SAM configuration, is needed to use the TOE as a security access module via the contact interface only. For this reason, the TOE generates and stores a set of cryptographic keys for different signature algorithms that can be used after appropriate authentication.

The TOE claims strict conformance to *[PP0059]*, but since in the SAM configuration the secure signature device is not used by a human technical details regarding the use of reference authentication data was added.

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

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 v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD), 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 v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) 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 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 *[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

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

NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) from cv cryptovision GmbH located in Gelsenkirchen, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), registered under the reference BSI-DSZ-CC-1149-V3-2023	A1
Platform	NXP JCOP4.5 P71, registered under the reference NSCIB-CC-2300127-01	226072
Applet	NXP eDoc Suite on JCOP4.5 P71 – cryptovision ePasslet Suite	4.0

To ensure secure usage a set of guidance documents is provided, together with the NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD). For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.

2.2 Security Policy

The TOE is a Java Card with a set of applets (NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite) configured to provide a secure signature creation device (SSCD) with key generation for the creation of legally binding qualified electronic signatures and qualified electronic seals as defined in the eIDAS regulation. To allow secure access to the signature functionality over the contactless interface, it provides an optional PACE mechanism to build up a secure channel for the verification authentication data (signature password/PIN or data derived from a user’s biometric characteristics).

The platform of the TOE is available with or without different biometric libraries, and thus also the TOE itself can be delivered without or with these biometric libraries. Details are described in the platform guidance.

2.3 Assumptions and Clarification of Scope

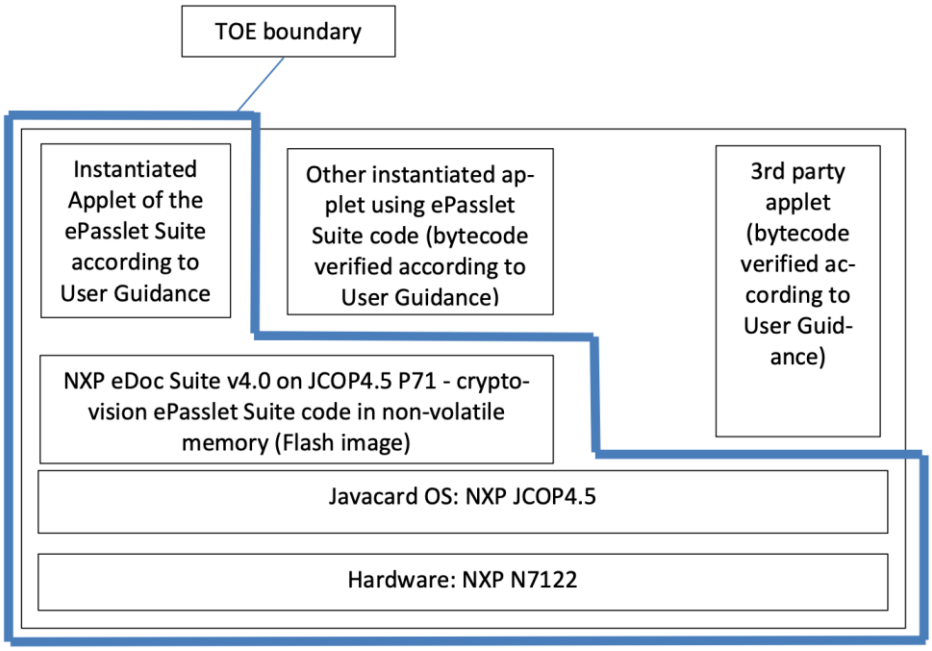
2.3.1 Assumptions

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

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information



The whole applet code resides in the Flash memory; the applets providing these different configurations are instantiated into Flash memory. Multiple configurations (and hence support for different applications) can be present at the same time by instantiating multiple applets with their distinct configurations.

A common combination could be an ICAO MRTD applet and an SSCD applet providing a travel application with LDS data and EAC authentication together with a signature application.

Via configuration the instantiated applets can be tied to the contactless and/or the contact interface, respectively.

2.5 Documentation

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

Identifier	Version
NXP eDoc Suite v4.0 on JCOP4.5 - cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with key generation dedicated to be used as Security Access Module (SAM) - Preparation Guidance (AGD_PRE_SAM), dated 26 February 2024	1.0.4
NXP eDoc Suite v4.0 on JCOP4.5 - cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with key generation dedicated to be used as Security Access Module (SAM) - Operational Guidance (AGD_OPE_SAM) , dated 26 February 2024	1.0.5
NXP eDoc Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation / key import Preparation Guidance (AGD_PRE) , dated 26 February 2024	1.0.8
NXP eDoc Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation / key import. Operational Guidance (AGD_OPE) , dated 26 February 2024	1.0.10

NXP eDoc Suite v4.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications. Guidance Manual, dated 22 January 2024	1.0.2

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

The underlying hardware and crypto-library test results are extendable to composite evaluations, because 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 provided samples and a test environment. The evaluators 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 technical report [JCOP-ETRfC] of the underlying platform.
- 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 4 weeks. During that test campaign, 33% of the total time was spent on Perturbation attacks and 67% on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- EAC-PACE TOE
- SSCD-KeyGen TOE

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 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD).

2.9 Evaluation Results

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 v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2**. 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_0059]*.

2.10 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 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 proprietary or non-standard algorithms, protocols and implementations: None

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The NXP eDoc Suite v4.0 on JCOP4.5 P71 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) Security Target, Version 2.0, Dated 27 February 2024 *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions 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
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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[EN419211-2]	EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
[ETR]	Evaluation Technical Report “NXP eDoc Suite v4.0 on JCOP4.5 P71 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)” – EAL5+, 24-RPT-174, Version 2.0, Dated 14 March 2024
[HW-CERT]	Certification Report, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1149-V3-2023
[HW-ST-Lite]	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) Security Target Lite, Rev. 1.8, dated 1 December 2023
[PLAT-CERT]	Certification Report JCOP 4.5 P71. Sponsor and developer: NXP Semiconductors Germany GmbH. Report number: NSCIB-CC- 2300127-01-CR. Version 1, dated 16 January 2024
[PLAT-ETRfC]	Evaluation Technical Report for Composition “NXP JCOP 4.5 P71” – EAL6+, 23- RPT-1350, version 2.0, dated 20 December 2023
[PLAT-ST-Lite]	JCOP 4.5 P71 Security Target Lite for JCOP 4.5 P71, Rev. 2.6, 11 December 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[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 2.6, 02 August 2022
[ST]	NXP eDoc Suite v4.0 on JCOP4.5 P71 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) Security Target, Version 2.0, Dated 27 February 2024
[ST-lite]	NXP eDoc Suite v4.0 on JCOP4.5 P71 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) Security Target Lite, Version 2.1, Dated 11 March 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)