# Certification Report

# EP-COS V3.0 Plain, EPCOSV30d

Sponsor and developer: ***NXP Semiconductors GmbH, Business Unit Security & Connectivity***
**Stresemannallee 101**
**22529 Hamburg**
**Germany**

Evaluation facility: ***Brightsight***
**Delftechpark 1**
**2628 XJ Delft**
**The Netherlands**

| | |
|---|---|
| Reportnumber: | **NSCIB-CC-127667-CR2** |
| Report version: | **1** |
| Projectnumber: | **NSCIB-CC-127667** |
| Author(s): | **Wouter Slegers** |
| Date: | **15 March 2017** |
| Number of pages: | **12** |
| Number of appendices: | **0** |

# Certificate

| | |
|---|---|
| Standard | Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408) |
| Certificate number | **CC-17-127667** |
| | TÜV Rheinland Nederland B.V. certifies: |
| Certificate holder and developer | **NXP Semiconductors GmbH, Business Unit Security & Connectivity**<br>**Stresemannallee 101, D-22529 Hamburg, Germany** |
| Product and assurance level | **EP-COS V3.0 Plain, EPCOSV30d,**<br>Assurance Package:<br>▪ EAL4 augmented with ALC_DVS.2 and ATE_DPT.2<br>Protection Profile Conformance:<br>▪ Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, 25th March 2009, registered under the reference BSI-CC-PP-0055-2009 |
| Project number | **NSCIB-CC-127667** |
| Evaluation facility | **Brightsight BV located in Delft, the Netherlands**<br>Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045) |

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

| | |
|---|---|
| Validity | Date of 1st issue : **14-02-2017** |
| | Date of 2nd issue : **17-03-2017** |
| | Certificate expiry : **14-02-2022** |

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

# CONTENTS:

TÜVRheinland®
Precisely Right.

## 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 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.

TÜVRheinland®
Precisely Right.

# 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 levels 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 EP-COS V3.0 Plain, EPCOSV30d. The developer of the EP-COS V3.0 Plain is NXP Semiconductors GmbH, Business Unit Security & Connectivity 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 Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to Part 1 of 'ICAO Doc 9303'.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 14 February 2017. The re-evaluation also took place by Brightsight B.V. and was completed on 13 March 2017 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]*.

The reason for the re-certification was a minor change to the evidence. The security evaluation re-used the evaluation results of the recently performed evaluation. The updated TOE identified in this report was assessed using the developers Impact Analysis Report (IAR). The IAR is intended to satisfy requirements outlined in the document Assurance Continuity: CCRA Requirements *[CCRA-AC]*. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes. The assessment indicated that the original evaluation results could be re-used and the Security Target *[ST]* and the public version of the Security Target *[ST-lite]* only needed editorially updating to include changes of the provided guidance documentation.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the EP-COS V3.0 Plain, 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 EP-COS V3.0 Plain 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 it meets the EAL4augmented (EAL4(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and ATE_DPT.2 (Testing: security enforcing modules).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the EP-COS V3.0 Plain, EPCOSV30d 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 EP-COS V3.0 Plain, EPCOSV30d from NXP Semiconductors GmbH, Business Unit Security & Connectivity located in Hamburg, Germany.

The TOE is comprised of the following main components:

| Delivery item type | Identifier and version |
|---|---|
| Hardware | P60D081PVB (P6021yVB configuration) with Crypto Library V3.1.2 on P60D081PVB |
| Software | IC Embedded Software (operating system) |
| | MRTD application BAC |

To ensure secure usage a set of guidance documents is provided together with the EP-COS V3.0 Plain. 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]/[ST lite]*, section “TOE life cycle”.

## 2.2 Security Policy

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to Part 1 ‘ICAO Doc 9303’.

## 2.3 Assumptions and Clarification of Scope

### 2.3.1 Assumptions

Detailed information on the assumption and threats can be found in the *[ST]* sections 3.2 and 3.3 respectively. Detailed information on the 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 Target of Evaluation (TOE) EP-COS V3.0 Plain is the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to the ICAO documentation.

The TOE is comprised of the following subsystems:

- the circuitry of the MRTD's chip P60D081PVB (P6021yVB configuration) with Crypto Library V3.1.2 on P60D081PVB
- the IC Embedded Software (operating system)
- the MRTD application BAC

Using this, the TOE provides an ISO 7816-4 file structure according to the ICAO 9303 specifications.

## 2.5 Documentation

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

| Identifier | Version |
|---|---|
| Personalization Guidance (AGD_PRE) EP-COS_V3.0_Plain | version 0.98, 27 February 2017 |
| Operational User Guidance (AGD_OPE) EP-COS_V3.0_Plain | version 0.97, 27 February 2017 |

## 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 SFR-enforcing module level. The testing was largely automated using proprietary test suites, mostly on the actual TOE and in exception cases on an emulator.

The hardware and crypto-library test results are extendable to composite evaluations, as this 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. The evaluators have witnessed the execution of the test suite by the developer, and performed a small number of test cases designed by the evaluator, addressing edge cases.

### 2.6.2 Independent Penetration Testing

The penetration tests are devised after performing the Evaluator Vulnerability Analysis. This analysis has followed the following steps. The reference for attack techniques against which smart card-based devices such as the TOE must be protected against is the document "Attack methods for smart cards" [JIL-AM]. Additional guidance for testing was provided by the certification body in the form of a number of questions regarding the TOE. The vulnerability of the TOE for these attacks has been analysed in a white box investigation conforming to AVA_VAN.3.

1. *Inventory of required resistance*
   This step uses the JIL attack list [JIL-AM] as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the TOE. Also the BSI attack list for RSA [RSA-BSI] has been used.

2. *Validation of security functionalities*
   This step identifies the implemented security functionalities and performs tests to verify the implementation and to validate proper functioning. (ATE)

3. *Vulnerability analysis*
   This step first gives an overview against which attacks the implemented security functionalities are meant to provide protection. Secondly in this step the design of the implemented security functionalities is studied. This also includes the security functionalities implemented in the hardware (cf. [HW-UG-021], [HW-ETRfC]). Thirdly, analysis is performed to determine whether the design contains vulnerabilities against the respective attacks of Step 1. (AVA)

4. *Analysis of input from other evaluation activities*
   This step first analyses the input from other CC-evaluation classes expressed as possible vulnerabilities. Secondly, the evaluators performed analysis of the TOE in its intended environment to check whether the developer vulnerability analysis provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance. (AVA)

5. *Design assurance evaluation*
   This step analyses the results from an attack perspective as defined in Step 1. Based on this design analysis the evaluators determine whether the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance. (AVA)

6. *Penetration testing*
   This step performs the penetration tests identified in Step 4 and Step 5. (AVA)

7. *Conclusions on resistance*
   The evaluators analyse the results of the penetration tests performed in Step 6. Based on this analysis the evaluators draw conclusions on the resistance of the TOE attackers possessing Enhanced-Basic attack potential.

No potential vulnerabilities within the attack potential were found not already covered by the underlying platform.

For extra assurance, several of the potential vulnerabilities beyond the attack potential were tested. The total test effort was 26 days, and consisted of one EMFI and three laser tests.

### 2.6.3 Test Configuration

Testing has been performed on the TOE as inlays, SO28, CLCC and DIL packages. The SO28 have been used for ATE developer tests; the inlays have been used for ATE independent and AVA tests; the DIL and CLCC packages have been used for AVA tests only. In all cases the samples have been delivered in locked state. The evaluators have run a script to bring the samples from the locked state to unlocked state and further on to the operational state. The ATE tests cover all life-cycle states of the TOE. The AVA tests target the operational state.

### 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.

## *2.7 Re-used evaluation results*

This security evaluation re-used the evaluation results of the recently performed evaluation which has been performed as a composite evaluation on the underlying hardware platform *[HW-CERT]* and crypto library *[CL-CERT]*. Sites involved in the development, production and delivery of the hardware and crypto library platform were re-used by composition. The site where the native operating system and application were developed, was audited on July 5th, 2016.

On 2 March 2017, NXP the developer of the EP-COS V3.0 Plain submitted an application form and Impact Analysis Report (IAR) to the NSCIB Certification Body requesting to issue a new certificate for their updated EP-COS V3.0 Plain product. The IAR is intended to satisfy the requirements outlined in the document 'Assurance Continuity: CCRA Requirements' *[CCRA-AC]*. In accordance with those requirements, the IAR describes the changes made to the recently certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The changes of the TOE can be categorized as a minor change to the evidence.

The assessment of the IAR by the evaluation lab in the *[ETR]* indicated that the changes have no security issues and that the original evaluation results could be re-used. The evaluation lab confirmed in the *[ETR]* that the original Vulnerability Analysis is still valid.

## 2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number EP-COS V3.0 Plain, EPCOSV30d.

## 2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the 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 EP-COS V3.0 Plain, EPCOSV30d, to be **CC Part 2 extended**[3]**, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and ATE_DPT.2**. This implies that the product satisfies the security technical requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, 25th March 2009, registered under the reference BSI-CC-PP-0055-2009.

## 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 (including the ICAO guidelines)

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 configuration of the TOE in its evaluated configuration.

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 implemented cryptographic algorithms was not rated in the course of this evaluation.

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

[3] The TOE is a composite TOE with a certified hardware platform. Claiming CC Part 2 extended is because the underlying platform claims CC Part 2 extended

# 3 Security Target

The Security Target EP-COS V3.0 Plain, Rev. 1.7, dated 27 February 2017 *[ST]* is included here by reference.

Please note that for the need of publication a public version (Security Target Lite EP-COS V3.0 Plain, Rev. 1.7, dated 27 February 2017) *[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:

| | |
|---|---|
| ICAO | International Civil Aviation Organisation |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| MRTD | Machine readable travel document |
| MRZ | Machine readable zone |
| NSCIB | Netherlands scheme for certification in the area of IT security |
| PP | Protection Profile |
| TOE | Target of Evaluation |

TÜVRheinland®
Precisely Right.

# 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 4, September 2012. |
| [CEM] | Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012. |
| [CCRA-AC] | Assurance Continuity: CCRA Requirements, CCRA Supporting Document, version 2.1, June 2012. |
| [CL-CERT] | Certification report. Crypto Library V3.1.x on P6021y VB, NSCIB-CC-15-66030-CR, dated 2 June 2016. |
| [CL-ETRfC] | ETR for Composite Evaluation Crypto Library V3.1.x on P6021y VB EAL6+/5+, version 7.0, dated 25 April 2016. |
| [CL-ST] | Crypto Library V3.1.x on P6021y VB Security Target, Rev. 1.4, 18-03-2016, Evaluation document, NSCIB-CC-15-66030, Public, Rev 1.4, dated 18 March 2016. |
| [ETR] | Evaluation Technical Report NXP EP-COS V3.0 Plain EAL4+, 17-RPT-051, version 3.0, dated 2017-03-09, and<br>Evaluation Report on IAR EPCOS v3.0 and EPCOS v3.0 Plain Re-certification, 17-RPT-112, version 1.0, dated 2017-03-09. |
| [HW-CERT] | Certification Report for NXP Secure Smart Card Controller P6021y VB including IC Dedicated Software, BSI-DSZ-CC-0955-2016, 17 March 2016. |
| [HW-ETRfC] | TÜVIT Evaluation Technical Report for Composite Evaluation (ETR COMP), v3, 12-02-2016, BSI-DSZ-CC-0955, P6021y VB, dated 12 February 2016. |
| [HW-ST] | NXP Secure Smart Card Controller P6021y VB, Security Target Lite, Rev. 0.93, 25-01-2016, Evaluation Document, BSI-DSZ-CC-0955, dated 25 January 2016. |
| [HW-UG-021] | NXP Secure Smart Card Controller P6021y VB Information on Guidance and Operation, Rev. 1.0, 28-08-2015, Guidance and Operational Manual, docstore number 323810. |
| [JIL-AM] | JIL, (Mandatory) Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.2, January 2013. |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015. |
| [ST] | Security Target EP-COS V3.0 Plain, Rev. 1.7, dated 27 February 2017. |
| [ST-lite] | Security Target Lite EP-COS V3.0 Plain, Rev. 1.7, dated 27 February 2017. |
| [ST-SAN] | ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006. |


(This is the end of this report).