Certification Report

Mercury ePassport v1.16

Sponsor and developer: ***Infineon Technologies AG***
Am Campeon 5
D-85579 Neubiberg
Germany

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

Reportnumber:	**NSCIB-CC-16-95781-CR**
Report version:	**1**
Project number:	**NSCIB-CC-16-95781**
Author(s):	**Wouter Slegers**
Date:	**14 February 2017**
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

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-16-95781**
	TÜV Rheinland Nederland B.V. certifies:
Certificate holder and developer	**Infineon Technologies AG** **Am Campeon 5, D-85579 Neubiberg, Germany**
Product and assurance level	**Mercury ePassport v1.16** Assurance Package: ▪ EAL4 augmented with ALC_DVS.2 (when BAC is used) ▪ EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 (when PACE is used) Protection Profile Conformance: ▪ When BAC is used: BSI-CC-PP-0055, Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, Issue 25.03.2009 ▪ When PACE is used: BSI-CC-PP-0068-V2-2011-MA-01, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, Issue 22.07.2014
Project number	**NSCIB-CC-16-95781-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** 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 issue : **16-02-2017**
	Certificate expiry : **16-02-2022**

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 would indicate 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 Mercury ePassport v1.16. The developer of the Mercury ePassport v1.16 is Infineon Technologies *AG* located in Neubiberg, 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 a contactless chip of an ePassport including the Mercury ePassport application. It is based on the requirements from the ICAO for machine readable travel documents, i.e. *[ICAO_9303_10]* and *[ICAO_9303_11].*

The security IC hardware is a M7892 D11 device certified under BSI-DSZ-CC-0891-v2-2016. It also contains firmware and asymmetric cryptographic libraries (ACL). Besides the hardware platform, the TOE contains the Mercury OS and the Mercury ePassport application (v1.16) that are placed on the hardware platform.

Depending whether BAC or PACE is used, the TOE is compliant with *[PP-BAC]* respectively *[PP-PACE]*.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 13 February 2017 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 Mercury ePassport v1.16, 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 Mercury ePassport v1.16 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 EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality when BAC is used. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures).
- the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality when PACE is used. 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 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 Mercury ePassport v1.16 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 Mercury ePassport v1.16, from Infineon Technologies *AG* located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	M7892 D11 platform	(See *[HW-ST]*)
	Hardware identification data	7633A301254EA097A6D57CFE3BD53A19
Software	Mercury ePassport application	afe6cd4c5de77b1d03d6315c11a3cbbe
	Mercury OS	c64640b66754c86185cbe70b274e193f
	Mercury pre-personalized file system	466d5bc7f87e18d513104a2832b28fba

To ensure secure usage a set of guidance documents is provided together with the TOE. 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 1.4.5.

2.2 Security Policy

As an ePassport implementing the specification from ICAO for machine readable travel documents, i.e. *[ICAO_9303_10]* and *[ICAO_9303_11],* compliant with *[PP-BAC]* and *[PP-PACE]*, the TOE security features in its operational use are:

- Only terminals possessing authorisation information (the shared secret MRZ optically retrieved by the terminal) can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal connected
- Averting of inconspicuous tracing of the travel document,
- Self-protection of the TOE security functionality and the data stored inside.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

Detailed information on the assumption and threats can be found in the *[PP-BAC]* and *[PP-PACE]* section 3 “Security Problem Definition” respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 4 “Security Objectives” of the *[PP-BAC]* and *[PP-PACE]*.

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 all TOEs compliant to the BAC protocol critically depend on the objectives for the environment for the inspection systems to be followed.

2.4 Architectural Information

The logical architecture of the TOE can be depicted as follows (based on *[ST]):*

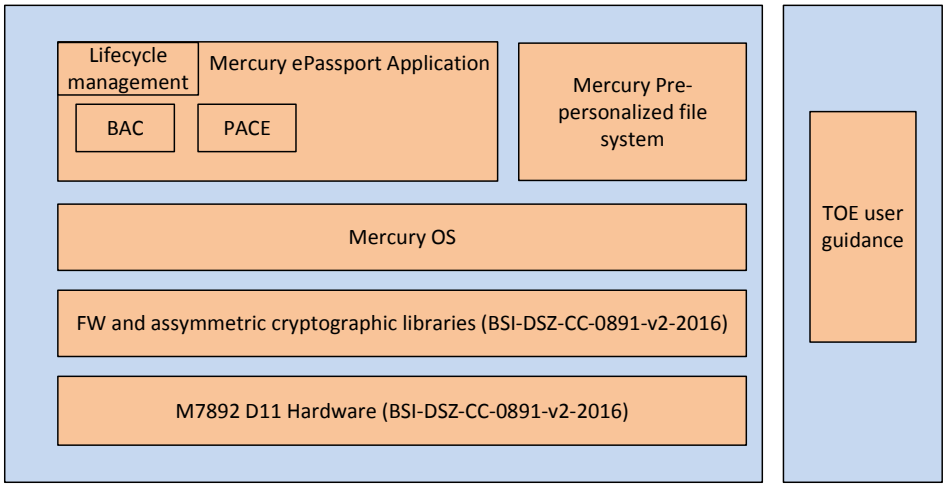

Figure 1. Logical architecture of the TOE.

The TOE has the following features (please note that this list is not exhaustive):

- Communication: ISO/IEC 14443 Type B (contactless)
- BAC mutual authentication scheme with session key agreement according to *[ICAO_9303_11]*
- PACE mutual authentication scheme with session key agreement according to *[ICAO_9303_11]*
- Commands for personalization of the ePassport

2.5 Documentation

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

Identifier	Version
Mercury: ePassport Data Book	V1.25
Infineon Technologies Mercury ePassport User Guide	V2.3

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

For the developer tests two types of test were used: white box (WB) testing and black box (BB) testing. The WB testing is performed on the same product as the TOE although, more functionality is available i.e., it is more open (EAC, more life cycle states, etc.). The BB testing is performed on the TOE. The actual TOE is used to test all that is specific for the TOE (correct functionality available, life cycle management conformant with the ICAO specifications, etc.).

For the evaluator tests, due to the high coverage by the developer, a limited set of independent tests confirming presence of security features and absence of unwanted functionality were performed.

2.6.2 Independent Penetration Testing

The penetration tests are devised after performing the Evaluator Vulnerability Analysis. 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 for BAC functionality and AVA_VAN.5 for PACE functionality.

In total 2 perturbation and 1 side channel tests were performed at AVA_VAN.5 level.

2.6.3 Test Configuration

Testing was performed on the final version of the TOE in its evaluated configuration.

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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that the remaining security level exceeds 100 bits after the best attack. So no exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

This is a new composite certification: direct re-use has been made of the certification of the underlying hardware platform (including crypto library). No evaluation results have been re-used.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE using site certificates. Sites involved in the development and production of the hardware platform were re-used by composition.

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 Mercury ePassport v1.16.

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 Mercury ePassport v1.16, to be **CC Part 2 extended**[3]**, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented**

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

with ALC_DVS.2 (when used with BAC) and **EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 (when used with PACE)**. This implies that the product satisfies the security technical requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the *[PP-BAC]* (when BAC is used) and *[PP-PACE]* (when PACE is used) registered and certified by BSI.

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 guidance for the administrator (personalizer) and the user (inspection system following 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 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 implemented cryptographic algorithms was not rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

[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 *[ST]* is included here by reference.

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
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MRZ	Machine Readable Zone
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 version 3.1 revision 1, and Part 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.
[ETR]	Evaluation Technical Report Mercury ePassport v1.16 EAL4+ (BAC) and EAL5+ (PACE), Version 7.0, Issue 9 February 2017.
[HW-CERT]	Certification report BSI-DSZ-CC-0891-V2-2016 for Infineon Security Controller, M7892 Design Steps D11 and G12, V1.0, 20 December 2016.
[HW-ETRfC]	Evaluation Technical Report for Composite Evaluation, v1, 2 December 2016.
[HW-ST]	M7892 Design Steps D11 and G12, revision 1.7, 16 November 2016.
[ICAO_9303_10]	International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC).
[ICAO_9303_11]	International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015 Part 11: Security Mechanisms for MRTD's.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
[PP-BAC]	BSI-CC-PP-0055: Machine Readable Travel Document with „ICAO Application”, Basic Access Control, Version 1.10, Issue 25.03.2009.
[PP-PACE]	BSI-CC-PP-0068-V2-2011-MA-01: Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, Issue 22.07.2014.
[ST]	Security Target Mercury ePassport v1.16, version 2.0, dated 2017-01-13.

(This is the end of this report).