

Certification Report

Mercury ePassport v2.20

Sponsor and developer: ***Infineon Technologies AG***
Am Campeon 1-15
85579 Neubiberg
Germany

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-146301-CR2**

Report version: **1**

Project number: **146301_2**

Author(s): **Andy Brown**

Date: **05 August 2020**

Number of pages: **12**

Number of appendices: **0**

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

CONTENTS:

Foreword	3
Recognition of the certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	7
2.1 Identification of Target of Evaluation	7
2.2 Security Policy	7
2.3 Assumptions and Clarification of Scope	7
2.4 Architectural Information	8
2.5 Documentation	8
2.6 IT Product Testing	9
2.7 Re-used evaluation results	9
2.8 Evaluated Configuration	10
2.9 Results of the Evaluation	10
2.10 Comments/Recommendations	10
3 Security Target	11
4 Definitions	11
5 Bibliography	12

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

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

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: <http://www.commoncriteriaportal.org>.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: <http://www.sogisportal.eu>.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Mercury ePassport v2.20. The developer of the Mercury ePassport v2.20 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 or M7892 P11 device certified under BSI-DSZ-CC-0891-V4-2019 or BSI-DSZ-CC-1105-2020, respectively. It also contains firmware and asymmetric cryptographic libraries (ACL). Besides the hardware platform, the TOE contains the Mercury OS and the Mercury ePassport application (v2.20) that are placed on the hardware platform.

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

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 14-08-2017. The re-evaluation also took place by Brightsight B.V. and was completed on 24-07-2020 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 changes are:

- Functional (minor) updates to the embedded software.
- Adding a new production site for the underlying hardware. The hardware produced in the new production site has received a new hardware certificate.

The security evaluation re-used 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 Mercury ePassport v2.20, 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 v2.20 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report [ETR]¹ for this product provides sufficient evidence that the TOE meets:

- the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality 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 5 [CEM], for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 [CC].

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

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

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Mercury ePassport v2.20 from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	M7892 Hardware (BSI-DSZ-CC-0891-V4-2019) including firmware and asymmetric crypto library	DF296F4C789F98C317DBFBB0536D7F92
	M7892 Hardware (BSI-DSZ-CC-1105-2020) including firmware and asymmetric crypto library	50FAFC994337EE7BA00D98638C689BD7
Software	Mercury OS	2017.03
		D3 92 D3 A0 2E 4E D6 B2 02 12 CA 06 EF A0 49 00
	Mercury ePassport application	B6 C2 0E 3B B4 89 06 58 95 5F 1C 9B AD 1F D7 1B
	Mercury pre-personalized file system	85 49 8B E1 55 71 43 F9 AA AA F1 D4 9B B7 2F 42

To ensure secure usage a set of guidance documents is provided together with the Mercury ePassport v2.20. 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

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

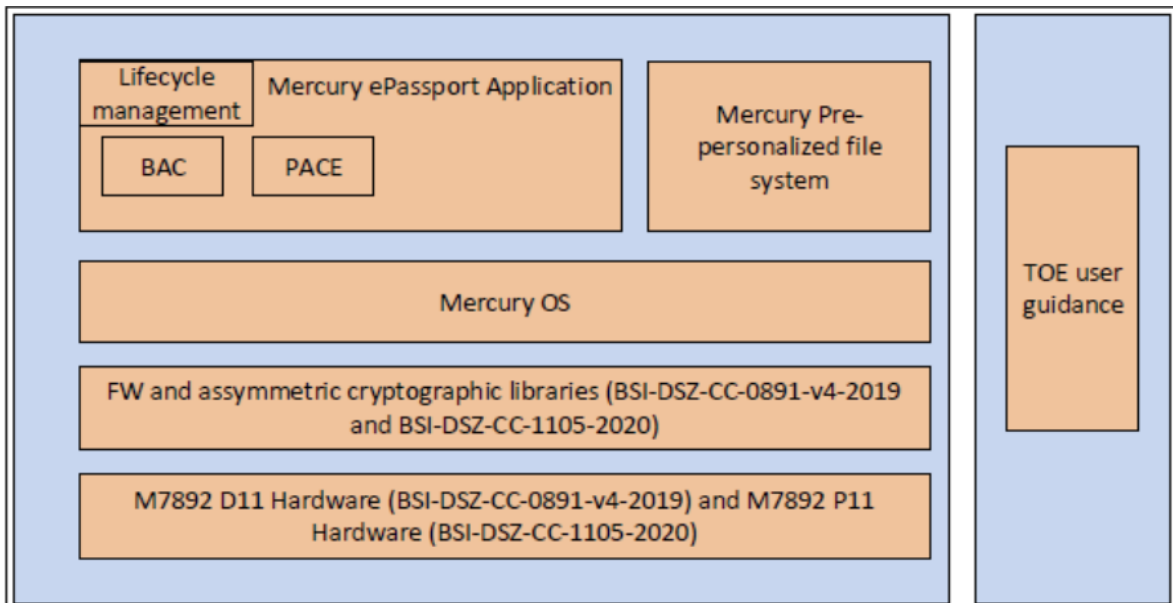


Figure 1 Logical architecture of the TOE.

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];
- Proprietary 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 section 10	v2.08
Infineon Technologies Mercury ePassport User Guide	v2.8

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 were 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]. 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. Since, no significant changes occurred compared to Mercury ePassport v2.10, and these changes did not have any negative security impact on the TOE and the vulnerability analysis, the Penetration Testing from the previous certification was repeated. For the Penetration Tests, samples including the P11 IC were used and the test results were compared against the test results from the previous evaluation (on samples with the D11 IC).

In total 1 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 re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use 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 re-used by composition.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 2 site certificates.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Mercury ePassport v2.20. The verification method of the TOE identifier is indicated in the User Guide referenced in section 2.5.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the [ETR] which references a 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 v2.20, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented 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 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).

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 cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>.

3 Security Target

The Security Target Mercury ePassport v2.20, Revision 3.5, 2020-07-15 [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, 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 Mercury ePassport v2.20, 20-RPT-165, v4.0, 17 July 2020.
- [HW-CERT-D11] Certification report BSI-DSZ-CC-0891-V4-2019 for Infineon Security Controller, M7892 Design Steps D11 and G12, V1.0, 19 December 2019
- [HW-CERT-P11] Certification report BSI-DSZ-CC-1105-2020 for Infineon Security Controller, M7892 Design Steps P11, V1.0, 30 June 2020
- [HW-ETRFc-D11] Evaluation Technical Report for Composite Evaluation, V2, 16 December 2019
- [HW-ETRFc-P11] Evaluation Technical Report for Composite Evaluation, V4, 02 June 2020
- [HW-ST-D11] M7892 Design Steps D11 and G12, revision 2.1, 25 November 2019
- [HW-ST-P11] M7892 Design Steps P11, revision 2.4, 23 April 2020
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
- [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] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-MA-01, Version 1.0.1, 22 July 2014, BSI.
- [ST] Security Target Mercury ePassport v2.20, Revision 3.5, 2020-07-15.

(This is the end of this report).