Certification Report

jePASS EAC V.1.1.4

Sponsor and developer: ***ST Microelectronics S.r.l***
Zona Industriale Marcianise SUD,
81025 Marcianise (CE),
Italy

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

Report number: **NSCIB-CC-0145427-CR**

Report version: **1**

Project number: **0145427**

Author(s): **Kjartan Jæger Kvassnes**

Date: **11 November 2020**

Number of pages: **11**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword **3**

Recognition of the certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **6**

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 6
2.4 Architectural Information 7
2.5 Documentation 7
2.6 IT Product Testing 7
2.7 Re-used evaluation results 8
2.8 Evaluated Configuration 8
2.9 Results of the Evaluation 8
2.10 Comments/Recommendations 9

3 Security Target **10**

4 Definitions **10**

5 Bibliography **11**

Foreword

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

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

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

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

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

Recognition of the certificate

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

International recognition

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

European recognition

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the jePASS EAC V.1.1.4. The developer of the jePASS EAC V.1.1.4 is ST Microelectronics S.r.l located in Marcianise, Italy 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 the composition of a software application with the secure IC STMicroelectronics ST31G480.

The TOE implements the Extended Access Control (EAC). The EAC consists of two parts, the Chip Authentication Protocol v.1 and the Terminal Authentication Protocol v.1.

The Chip Authentication Protocol v.1 authenticates the TOE to the inspection system and establishes secure messaging which is used by Terminal Authentication Protocol v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication Protocol v.1 can only be performed if Chip Authentication Protocol v.1 has been successfully executed.

The Terminal Authentication Protocol v.1 consists of the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The TOE implements Active Authentication. Keys for Active Authentication can be loaded into the TOE. These operations take place at personalization time

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11 November 2020 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 jePASS EAC V.1.1.4, 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 jePASS EAC V.1.1.4 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. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), ATE_DPT.2 (Testing: security enforcing modules) 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 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 jePASS EAC V.1.1.4 from ST Microelectronics S.r.l located in Marcianise, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST31G480 IC	D01
	NESLIB cryptographic library	6.2.1
Software	Java Card operating system	1.1.4
	jePASS MRTD applet	1.1.4

To ensure secure usage a set of guidance documents is provided together with the jePASS EAC V.1.1.4. Details can be found in section 2.5 of this report. The ST31G480 IC D01 is the same version as the one mentioned in the IC certificate [HW-CERT] which was confirmed to be identical for the scope of the composite TOE when applying the updated guidance in [HW-SUR].

2.2 Security Policy

The TOE is a javacard applet implementing the machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) programmed according to the Logical Data Structure (LDS) and implementing the advanced security methods Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), Chip Authentication (CA) and the Active Authentication (AA) as described in the 'ICAO Doc 9303' [ICAO_9303].

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 10.2 of the *[ST-lite]*.

2.3.2 Clarification of scope

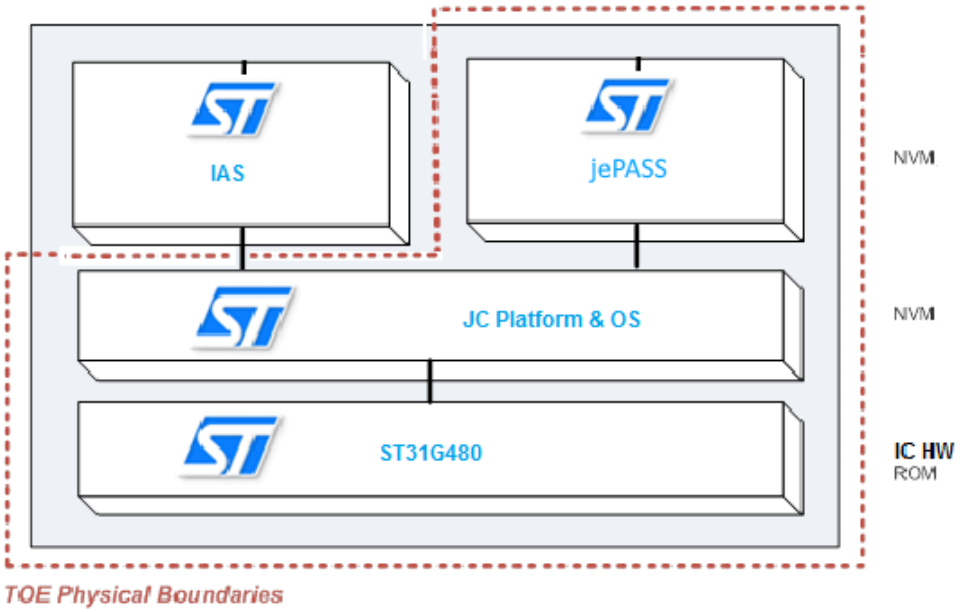
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

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 TOE is a contact/contactless chip and comprises the following elements:

- the STM IC ST31G480 Security Integrated Circuit with dedicated software and embedded cryptographic library.
- the Java CardTM Operating System v.1.1.4
- the TOE javacard applet jePASS v.1.1.4 implementing the machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO).

2.5 Documentation

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

Identifier	Version
jePASS Operational User Guidance	Revision G, 27 October 2020
jePASS Preparative Procedure	Revision H, 27 October 2020

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

Tests are performed as "System Test" using "Black Box" approach. If needed, "Grey Box" approach is also used. The developer tests are performed in a way that the TSF security requirements and respective interfaces are completely covered.

Separate test plan document is provided for each TSF. Both the application as well as the OS are addressed.

The underlying hardware and crypto-library test results are extendable to composite evaluations, as the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The sample strategy for the test witnessing is to repeat a small number of test cases from each of the different test plans, covering the standard ICAO testing, additional ICAO proprietary APDU testing, and OS level 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. An important source for assurance in this step is the technical report [ETRfC-HW] and the [HW-SUR] 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 overall testing effort was 2 weeks, which corresponds to the total duration of two perturbation attacks.

2.6.3 Test Configuration

The TOE was tested in the following configurations:

- jePASS v1.1.3.

The difference between version 1.1.3 and 1.1.4 was identified to be one single line of code and a code review determined that the change would not affect the results of the penetration testing and therefore these test results are valid for the final version of the evaluated TOE (v1.1.4).

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

2.7 Re-used evaluation results

There is no re-se of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number jePASS EAC V.1.1.4.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the jePASS EAC V.1.1.4, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.** This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims strict conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation.

3 Security Target

The jePASS EAC Security Target, Rev F, 27 October 2020 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation
CA	Chip Authentication
EAC	Extended Access Control
eMRTD	electronic MRTD
ICC	Integrated Circuit Card
JIL	Joint Interpretation Library
MRTD	Machine Readable Travel Document
PACE	Password Authenticated Connection Establishment
RNG	Random Number Generator
SM	Secure Messaging
TA	Terminal Authentication

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 STM jePASS V1.1.3 – EAL4+, 20-RPT-378, version 5.0, 11 November 2020.

[HW-CERT] Rapport de certification ANSSI-CC-2019/12, ST31G480 D01 including optional cryptographic library NESLIB v6.2.1, and optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6.

[HW-ETRfC] ETR for composition ST31G480, Revision 1.3.

[HW-ST] ST31G480 D01 Security Target, Revision D01.3.

[HW-SUR] Rapport de surveillance, ANSSI-CC-2019/12-S01, ST31G480 D02, 23 July 2020.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, Part 11 Security Mechanisms for MRTDs and Part 12 Public Key Infrastructure for MRTDs , Seventh Edition, 2015, International Civil Aviation Organization.

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

[PP] Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE Version 1.3.2, 05 December 2012, registered under the reference BSI-CC-PP-0056-V2-2012-MA-02.

[ST] jePASS EAC Security Target, Rev F, 27 October 2020.

[ST-lite] jePASS EAC Security Target Lite, Rev C, 27 October 2020.

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

(This is the end of this report).