TrustCB B.V.

TRUST AND VERIFY

Certification Report

ePass Applet on JCOP 4 C1

Sponsor: ***Veridos GmbH, Identity Solutions by Giesecke+Devrient and Bundesdruckerei***
Prinzregentenstraße 161
81677 Munich
Germany

Developer: ***Giesecke+Devrient Mobile Security GmbH***
Prinzregentenstraße 161
81677 Munich
Germany

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-2300097-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300097-01**
Author(s):	**Wim Ton**
Date:	**20 December 2023**
Number of pages:	**12**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 ePass Applet on JCOP 4 C1. The developer of the ePass Applet on JCOP 4 C1 is Giesecke+Devrient Mobile Security GmbH located in München, Germany and Veridos GmbH, Identity Solutions by Giesecke+Devrient and Bundesdruckerei 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 Target of Evaluation (TOE) is an electronic passport representing a smart card implementing [ICAO_9303_10], [ICAO_9303_11], [TR-03110_1] and [TR-03110_3].

This smart card / passport application provides a travel document containing the related user data as well as data needed for authentication with BAC, PACE, EAC or AA protocols (incl. PACE/BAC passwords).

The application is intended to be used by governmental organisations as a machine-readable travel document (MRTD).

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 20-12-2023 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 ePass Applet on JCOP 4 C1, 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 ePass Applet on JCOP 4 C1 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 following assurance requirements:

- The assurance level for the TOE is EAL5 augmented (EAL5+) with the components ALC_DVS.2 and AVA_VAN.5 in case PACE is used and EAC is not used and conformance to [PP_SAC] is claimed.
- The assurance level for the TOE is EAL5 augmented (EAL5+) with the components ALC_DVS.2 and AVA_VAN.5 in case PACE and EAC are used and conformance to [PP_EAC] is claimed.
- The assurance level for the TOE is EAL4 augmented (EAL4+) with the components ALC_DVS.2 and ATE_DPT.2 in case BAC is chosen as authentication method and conformance to [PP_BAC] is claimed.

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 NSCIB Certified Products list. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the ePass Applet on JCOP 4 C1 from Giesecke+Devrient Mobile Security GmbH located in München, Germany.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Hardware	NXP N7121	B1, R4 configuration
Platform	On-chip software	9.2.3.0
	Flashloader OS	1.2.5
	System Mode OS	13.2.3.0
	JCOP 4 P71	v4.7 R1.02.4
Software	ePass Applet	C1, v1.0 (build 11)

To ensure secure usage a set of guidance documents is provided, together with the ePass Applet on JCOP 4 C1. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 2.3.

2.2 *Security Policy*

The TOE is an eMRTD and encompasses the following features:

- During the Personalisation phase:
    - authentication protocol;
    - 3DES, AES128, AES192 and AES256 Global Platform secure messaging;
    - access control;
    - initialisation of the LDS;
    - data loading;
    - Secure import and/or on-chip generation of Chip Authentication key pairs for CAv1;
    - Secure import and/or on-chip generation the AA key pair;
    - life-cycle phase switching to operational phase.
- During the Operational phase:
    - Basic Access Control (BAC)
    - Password Authenticated Connection Establishment (PACE)
    - Active Authentication (AA)
    - Chip Authentication v1 (CAv1)
    - After CAv1: Read access to the holder’s data stored in the TOE using secure messaging with 3DES, AES128, AES192, or AES256.

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 3.4.7 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 personalised must perform proper and safe personalisation 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

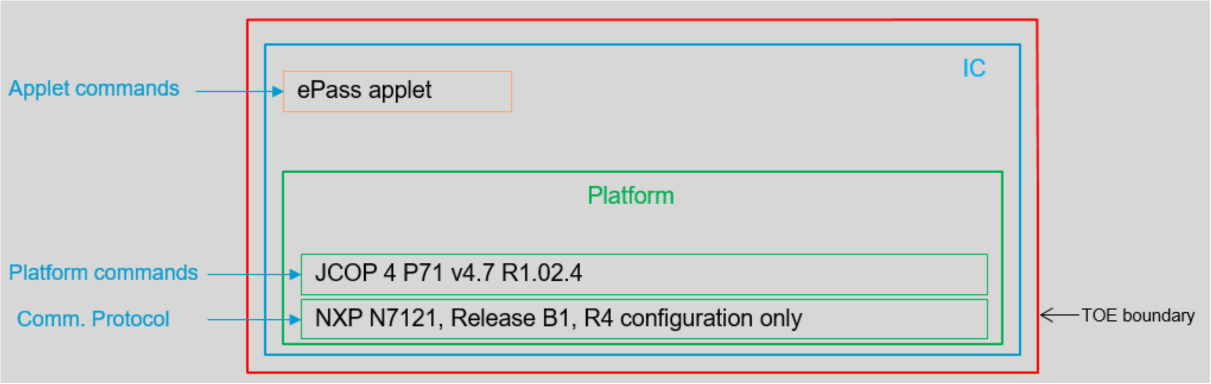

Figure 1 TOE boundary

2.5 Documentation

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

Identifier	Version
Guidance Documentation ePass Applet on JCOP 4 C1, Giesecke & Devrient	0.3
Guidance Documentation for the Usage Phase ePass Applet on JCOP 4 C1	0.2
EPASS Applet EPASS10-200 Personalization Concept, Giesecke & Devrient	1.3
EPASS Applet EPASS10-200 Usage Phase Commands, Giesecke & Devrient	1.3
Guidance Documentation for the Initialization and Personalization Phase ePass Applet on JCOP 4 C1, Giesecke & Devrient,	0.5
JCOP 4 P71, User manual for JCOP 4 P71, NXP DocNo 469543	4.3

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

Tests that are testing different parts of the functionality of the TOE were selected for witnessing. The tests were running at the network of the developer and videos of the tests were shared and they were analysed by the evaluator.

A sample of tests was witnessed with the following approach:

- Identify test samples (TOE and underlying platform)
- Check test environment
- Check tools and scripts used
- Witness of actual testing

The tests for the most important functionality of the ePass applet: BAC, PACE, Chip Authentication and Terminal Authentication and the different types of test (smoke, system, performance) were witnessed by the evaluator.

2.6.2 Independent penetration testing

Potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and from information in 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 2.75 weeks. During that test campaign, 36% of the total time was spent on Perturbation attacks, and 64% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]* chapter 3.4.1.

The evaluator testing and penetration testing was performed on the TOE in the operational life-cycle state with applet instance configurations specified in the Security Target *[ST]*.

The TOE was tested in the following configuration:

- TOE instantiated on the JCOP platform
- Using T=0, T=1 (ISO/IEC 7816) and T=CL (ISO/IEC 14443)

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.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by the use of 4 Site Technical Audit Reports.

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 ePass Applet on JCOP 4 C1.The version of the EPASS Applet is available in FCI information from the Select Command in tag DF76 and is “EPASS10-200-100-V100-0011”.

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 ePass Applet on JCOP 4 C1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of:

EAL4 augmented with ALC_DVS.2 and ATE_DPT.2 in case BAC is chosen as authentication method whereby conformance to [PP_BAC] is claimed and

EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5 in case PACE is chosen as authentication method whereby conformance to [PP_SAC] is claimed and

EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5 in case PACE and EAC are chosen as authentication methods whereby conformance to [PP_EAC] is claimed.

This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

This ST claims strict conformance

- to [PP_BAC], if a BIS chooses BAC as authentication method

- to [PP_SAC], if a BIS chooses PACE as authentication method

- to [PP_EAC], if an EIS choses PACE as authentication method and additionally uses Extended Access Control, which consists of two parts:

(i) the Chip Authentication Protocol Version 1 (v.1) and
(ii) the Terminal Authentication Protocol Version 1 (v.1) as defined in TR-03110_1.

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>, which are out of scope as there are no security claims relating to these.

3 Security Target

The Security Target ePass Applet on JCOP 4 C1, Version 1.3, 19 December 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAM	Chip Authentication Mapping
CGA	Certificate Generation Application
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DCAP	Dutch Conformity Assessment Program
DES	Data Encryption Standard
CVCA	Country Verifying Certification Authority
DFA	Differential Fault Analysis
EAC	Extended Access Control
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EIS	Extended Inspection System
EMA	Electromagnetic Analysis
eMRTD	electronic MRTD
FCI	File Control Information
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LAN	Local Area Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure

RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
TA	Terminal Authentication
TCP	Transmission Control Protocol
TRNG	True Random Number Generator

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
[ETR]	Evaluation Technical Report “Veridos ePass applet on JCOP4 C1” – EAL4/5, 23-RPT-1060, v4.0, 20 December 2023
[JC-CERT]	Assurance Continuity Maintenance Report JCOP 4 P71, NSCIB-CC-180212-5MA1, 23.01.2023
[JC-ETRfC]	Evaluation Technical Report for Composition NXP “JCOP 4 P71” – EAL6+, 19-RPT-177 v14.0, 14 September 2022
[JC-ST]	JCOP 4 P71 Security Target Lite, Security Target for JCOP 4 P71/SE050, Rev. 4.11, 03.01.2023, NXP Semiconductors
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_BAC]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009
[PP_EAC]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, registered under the reference BSI-CC-PP-0056-V2-2012
[PP_SAC]	Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0.1, 22 July 2014, registered under the reference BSI-CC-PP-0068-V2-2011-MA-01
[ST]	Security Target ePass Applet on JCOP 4 C1, Version 1.3, 19 December 2023

(This is the end of this report.)