Certification Report

Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE

Sponsor:	***Veridos GmbH, Identity Solutions by Giesecke+Devrient and Bundesdruckerei*** **Prinzregentenstr. 161** **1677 München** **Germany**
Developer:	***cv cryptovision GmbH*** **Munscheidstr. 14** **45886 Gelsenkirchen** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300087-01**
Report version:	**1**
Project number:	NSCIB-**2300087-01**
Author(s):	**Wim Ton**
Date:	**12 January 2024**
Number of pages:	**13**
Number of appendices:	**0**

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.

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 Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE. The developer of the Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE is cv cryptovision GmbH located in Gelsenkirchen, Germany and Veridos GmbH, Identity Solutions by Giesecke+Devrient and Bundesdruckerei acts 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 Java Card (Veridos Suite v4.0 - cryptovision ePasslet Suite) configured to provide a contactless integrated circuit chip containing components for a machine-readable travel document (MRTD chip). After instantiation and configuration of the according configuration it can be programmed according to the Logical Data Structure (LDS) and provides the Basic Access Control according to the ICAO document [ICAODoc]. The TOE is built upon a certified SmartCafe Expert 8.0 C2 Javacard OS Card.

The TOE has been evaluated by SGS Brightsight B.V. | located in Delft, The Netherlands. The evaluation was completed on 16-11-2023 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 Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE, 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 Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), and AVA_VAN.5 (Resistant against a high attack potential).

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 Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE from cv cryptovision GmbH located in Gelsenkirchen, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IFX SLC37GDA512	0xD1,0xE,0xE0,0xE2
Platform	SmartCafe Expert 8.0	C2
Software	Veridos Suite v4.0 - cryptovision ePasslet Suite	ver 0x0405
Configuration	ePasslet4.0/SSCD	ver 0x0401, rev 0x49E2

To ensure secure usage a set of guidance documents is provided, together with the Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE. For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.7.

2.2 Security Policy

eMRTD

The TOE in the **PACE configuration** 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:
  - Password Authenticated Connection Establishment (PACE)
  - Active Authentication (AA)
  - Chip Authentication v1 (CAv1)
  - After CAv1: restart ICAO secure messaging in 3DES, AES128, AES192, or AES256 cipher mode.

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 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 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

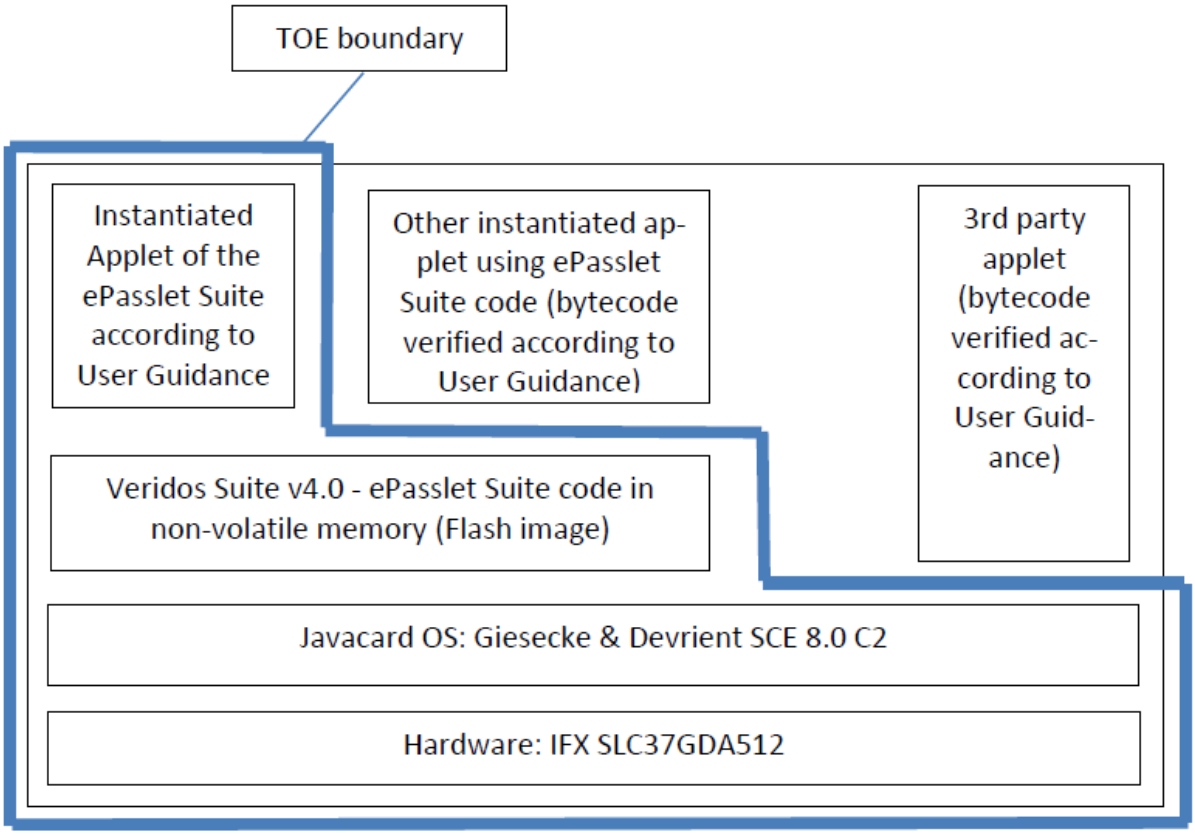

Figure 1 TOE components.

No applets that could uniquely identify a TOE instance without proper authentication shall be present in the “Operational use” life cycle phase. See AGD_PRE chapter 2.6.1.

2.5 Documentation

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

Identifier	Version
Guidance Manual	1.0.5
Preparation Guidance (AGD_PRE)	1.0.12

Operational Guidance (AGD_OPE)	1.0.11

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 performed extensive testing on the functional specification, using a specialized 3rd party tool to test the conformance to ICAODoc and TR-03110.

The developer performed extensive testing on functional specification of the ePasslet suite using an internal tool.

The average test coverage for instructions is 87% and for branches 77%. The developer explained to the evaluator those test cases where the coverage was below 85%.

Testing was executed on a simulator and on the target hardware.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced 10 of the developer tests, as well as 2 test cases designed by the evaluator.

2.6.2 Independent penetration testing

The total test effort expended by the evaluators was 4 weeks. During that test campaign, 20% of the total time was spent on perturbation attacks, 20% on side-channel testing, and 60% on software attacks.

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]*.

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

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.

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 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the site involved in the development and production of the TOE, by use of a Site Technical Audit Report *[STAR]*.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE. Before the operational state, the user can verify the TOE version as described in AGD_PRE chapter 2.5.3.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and a Site Technical Audit Report for the site *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the Veridos Suite v4.0 cryptovision ePasslet Suite Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.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 Profiles *[PP_56 and [PP_68]*.

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.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE Security Target, Version 1.8, 7 Nov 2023 *[ST]* is included here by reference.

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

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
CA	Chip Authentication
CAM	Chip Authentication Mapping
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
CVCA	Country Verifying Certification Authority
EAC	Extended Access Control
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
eMRTD	electronic MRTD
IC	Integrated Circuit
ISD	Issuer Security Domain
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
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
PUK	PIN Unblocking Key
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SCD	Signature Creation Device
SCP	Secure Channel Protocol

SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
SVD	Signature Verification Device
TA	Terminal Authentication
TOE	Target of Evaluation
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
[PLAT-CERT]	Certification Report Sm@rtCafé® Expert 8.0 C2, NSCIB-CC-2300005-01-CR, version 1, 24 May 2023
[PLAT-MAINT]	Assurance Continuity Maintenance Report Sm@rtCafé® Expert 8.0 C2, Report number: NSCIB-CC-2300005-01-MA, version 1, 18 September 2023
[PLAT-ETRfC]	Evaluation Technical Report for Composition “Sm@rtCafé® Expert 8.0 C2” – EAL6+ Recertification, SGS Brightsight, 23-RPT-398, Version 3.0, 10 May 2023
[PLAT-ST]	Sm@rtCafé® Expert 8.0 C2 Veridos Security Target, Version 4.2, 3 Aug 2023
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report “Veridos Suite v4.0 - cryptovision ePasslet Suite” –EAL4+/EAL5+, 23-RPT-850, Version 4.0, 16 November 2023
[HW-CERT]	Certification Report BSI-DSZ-CC-1107-V3-2022 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACLv3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and guidance from Infineon Technologies AG, 16 May 2022
[HW-ST]	Security Target Lite BSI-DSZ-CC-1107-V3-2022, Version 4.3.1, 2022-05-10, “IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite”, Infineon Technologies AG
[JIL-AAPS]	JIL, Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_56]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012

[PP_68]	Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01
[ST]	Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE Security Target, Version 1.8, 7 Nov 2023
[ST-lite]	Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine-Readable Electronic Documents „ICAO Application", Extended Access Control with PACE Security Target Lite, Version 1.8, 7 Nov 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	23-RPT-538, Site Technical Audit Report - Cryptovision Gelsenkirchen, version 1.0, 9 May 2023

(This is the end of this report.)