TÜVRheinland®
Precisely Right.

Certification Report

CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential

Sponsor and developer: ***IDEMIA***
2 Place Samuel de Champlain,
92400 Courbevoie,
France

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

Report number: **NSCIB-CC-200736-CR**

Report version: **1**

Project number: **200736**

Author(s): **Denise Cater**

Date: **07 January 2020**

Number of pages: **14**

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 5 (ISO/IEC 15408)
Certificate number	**CC-20-200736**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**IDEMIA** **2 Place Samuel de Champlain, 92400 Courbevoie, France**
Product and assurance level	**CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential** Assurance Package: ▪ EAL4 ALC_DVS.2, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 Protection Profile Conformance: ▪ Machine readable travel documents with "ICAO Application", Basic Access control, registered under the reference BSI-PP-0055 v1.10 25th March 2009
Project number	**200736**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (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 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. 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 1st issue : **07-01-2020** Certificate expiry : **07-01-2025**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

R. de Jonge, Managing director
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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, 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.

eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential. The developer of the CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential is IDEMIA located in Courbevoie, France 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 consists of a CombICAO Applet product in BAC and CA configuration composed with the certified underlying IDEMIA Java Card ID-ONE Cosmo V9 Essential. The product is designed to support the usage as an eMRTD, as per [ICAO_9303].

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO_9303].

The Chip Authentication defined in [TR_03110] or [ICAO_9303] is a security feature which is optionally supported by the TOE. This TOE addresses the Chip Authentication as an alternative to the Active Authentication stated in [ICAO_9303]. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 12 December 2019 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 CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential, 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 CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential 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), ADV_FSP.5 (Complete semi-formal functional specification with additional error information), ADV_INT.2 (Well-structured internals), ADV_TDS.4 (Semiformal modular design), ALC_CMS.5 (Development tools CM coverage), ALC_TAT.2 (Compliance with implementation standards) and ATE_DPT.3 (Testing: modular design).

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]*.

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

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SLC32GDL400G3 SLC32GDA400G3 SLC32GDA348G3 SLC32GDL348G3	IFX_CCI_000005
	SLC32PDL400	IFX_CCI_000008 IFX_CCI_000014
	Software Library - HSL	V01.22.4346-SLCx2_C65.lib
	Software Library - MCS (Mifare lib)	V02.03.3446
	Java Card Platform - ID-ONE COSMO V9 ESSENTIAL	SAAAAR 089233
Software	CombICAO applet	SAAAAR 203297

To ensure secure usage a set of guidance documents is provided together with the CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential. Details can be found in section “Documentation” of this report.

2.2 Security Policy

The TOE is delivered during the preparation phase after which the pre-personalisation and personalisation are performed.

The Pre-personalisation consists of:

- Authentication and secure channel using the in the certified platform implemented GP functionality using SCP02 and SCP03,
- Initialization of the TOE,
- Loading Personalization Agent keys in encrypted form,
- Storing the Initialization and Pre-Personalization data in audit records.

The Personalisation consists of:

- Authentication and secure channel using the in the certified platform implemented GP functionality using SCP02 and SCP03,
- Configuration of the TOE,
- Load user data,
- Configure SM level for biometrical data access,
- Load Chip Authentication keys in encrypted form,
- Set TOE life cycle to Operational Use phase.

See the *[ST]* for details, including section 1.3.6 of *[ST]* for details of the TOE lifecycle.

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 3.3 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.

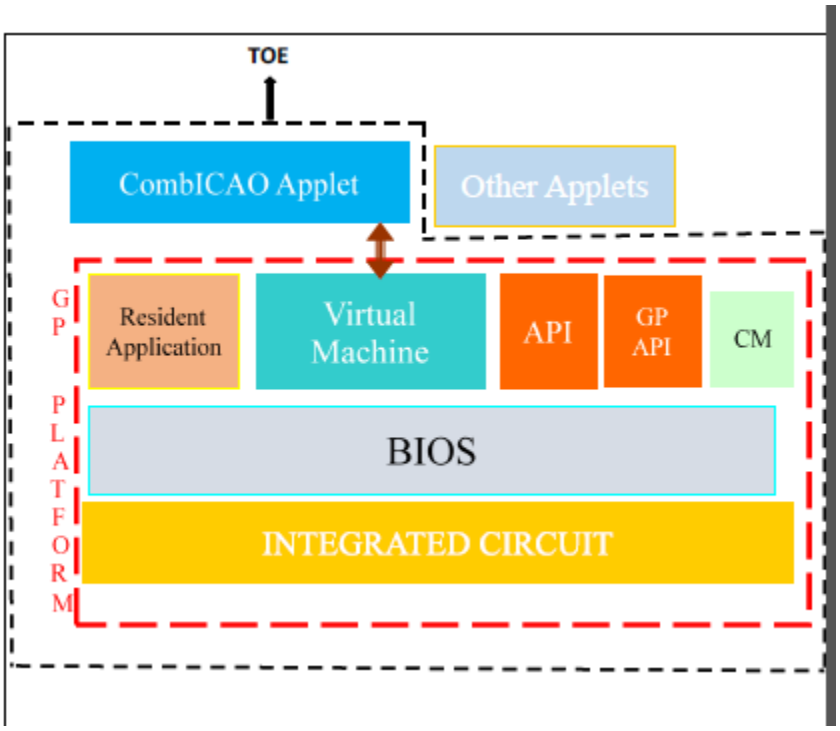
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is 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 consists of an applet and the certified Java Card platform (Cosmo v9 Essential) that can be configured to be used as an eMRTD as specified in *[ST]*. The logical architecture of the TOE can be depicted as follows:



The TOE provides the following features in operational phase

- BAC as defined in [ICAO 9303],
- CA version 1 part of EACv1 as defined in [TR_03110].

The Personalization and Operational phases are summarised in “Security Policy” section above.

2.5 Documentation

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

Identifier	Version
FQR 220 1306 - CombICAO Applet – AGD_PRE	Ed 8.
FQR 220 1307 - CombICAO Applet – AGD_OPE	Ed 9
Secure acceptance and delivery of sensitive element - FQR 110 8921	Ed 1
ID One Cosmo V9.0 Essential Reference Guide, FQR 110 8823	Ed 5
ID One Cosmo V9.0 Essential - Pre-Perso Guide, FQR 110 8797	Ed 5
ID-One Cosmo V9 Application Loading Protection Guidance, FQR: 110 8798	Ed 2
ID-One Cosmo V9 Applet Security Recommendations, FQR: 110 8794	Ed 4

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 has performed exhaustive testing on functional specification, subsystem and SFR-enforcing module level. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values. The Developer used a combination of test tools to test the TOE, including use of a commercial test bench from Keolabs/Scriptis, to test the operational behaviour of the TOE according to the [TR_03110] and [ICAO-9303] conformity test specifications. These conformity tests cover all eMRTD configurations of the TOE.

As the testing was automated the evaluator selected a small sample of tests to verify the correctness of the developer testing. All test results were as expected. Because no gaps could be identified in the developer testing evidence the evaluator devised a set of five (5) tests aiming to verify a part of the preparatory guidance and the access conditions.

For the independent functional testing performed by the evaluators, the developer provided samples and a test environment.

2.6.2 Independent Penetration Testing

The vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the attack list in [JIL_AM]. An important source for assurance against attacks in this step is the [HW_ETRfc] of the underlying platform; no additional potential vulnerabilities were concluded from this.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. All potential vulnerabilities were found to be not exploitable due to an impractical attack path for the TOE in its evaluated configuration..

2.6.3 Test Configuration

The following test benches were used for witness of developer testing:

- Oberthur Testing Framework v 1.7.2.1 (Including Python)
- Keolabs eMRTD Applicative Test Suite v 06.00 - Accreditation testing

The TOE was tested in the following configurations:

- T1; {for T=1, T=CL, and Dual executions; SCP0300 Configuration}
- T0; {for T=0 executions; SCP0300 Configuration }
- T1;USE_SCP02; {for T=1, T=CL, and Dual executions; SCP0255 Configuration }
- T0;USE_SCP02; {for T=0 executions; SCP0255 Configuration }

For the listed configurations the TOE is in Pre-personalization stage. The TOE is configured and personalized for each test of the Oberthur testing framework.

For the KEOLABS test suite, all tests are performed in the operational life-cycle state, and do not allow TOE identification. These samples are personalised according to the ePassport profiles mentioned in the ATE.

For evaluator independent testing, the TOE was tested in the following configurations:

- Configuration 1: Personalization stage with the eMRTD applet installed.
- Configuration 2: eMRTD.

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 vulnerability analysis.

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 Evaluated Configuration

The TOE is defined uniquely by its name and version number CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] and 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 CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 ALC_DVS.2, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3**. 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]*.

2.9 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 CombICAO Applet Security Target BAC and CA, FQR 110 8780, ed 10 *[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:

BAC	Basic Access Control
CA	Chip Authentication
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TA	Terminal Authentication
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.
[CR_PP]	Certification Report BSI-PP-0055-2009 for Machine readable travel documents with “ICAO Application” Basic Access control, version 1.10, 07 May 2009
[ETR]	Evaluation Technical Report CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential, 19-RPT-140, Version 5.0, 12 December 2019.
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015 – Security Mechanisms for MRTDs
[HW-CERT]	NSCIB-CC-200833-MA, v1, 01 August 2019
[HW-ETRfC]	Evaluation Technical Report for Composition ID-ONE COSMO V9 ESSENTIAL – EAL5+, 18-RPT-647, v6.0, 29 July 2019
[HW-ST]	SCYLLA Security Target, FQR 110 8779, Ed2
[JIL_AM]	Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.3, April 2019
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Machine readable travel documents with “ICAO Application”, Basic Access control, registered under the reference BSI-PP-0055 v1.10 25th March 2009
[ST]	CombICAO Applet Security Target BAC and CA, FQR 110 8780, ed 10.
[ST-lite]	CombICAO Applet in BAC and CA configuration on Cosmo V9 - Public Security Target, FQR 110 9316, Ed 3
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.
[TR_03110]	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, version 2.10, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

(This is the end of this report).