Certification Report

IDeal Drive DT V3.1 on Cosmo V9.1

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-0286910-CR**

Report version: **1**

Project number: **0286910**

Author(s): **Denise Cater**

Date: **16 February 2021**

Number of pages: **13**

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

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 IDeal Drive DT V3.1 on Cosmo V9.1. The developer of the IDeal Drive DT V3.1 on Cosmo V9.1 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 is the IDeal Drive DT v3.1, a Smart Tachograph second generation card compliant to the European Union regulation 2014/165 and its Commission implementation [EU – 2016/799] amended by [EU – 2018/502] related to digital tachograph generation 1.. The TOE is also a Digital Tachograph first genera\on card compliant to the European Union regulation [EU 1360/2002].

The TOE is an Integrated Circuit and its embedded software, composed of the Tachograph Java Card applet on top of a Java Card Open Platform ID-One Cosmo v9.1.

The TOE can be used in a recording equipment (or Vehicle Unit) of both Generation 1 as well as Generation 2. The TOE supports a single Tachograph Applet that provides both Generation 1 and Generation 2 functionalities with two configurations:

1. Configuration 1: Supporting Generation 1 only functionalities (compliant to [PP-GEN1]).
2. Configuration 2: Supporting both Generation 1 and Generation 2 functionalities (compliant to [PP-GEN2]).

The TOE can be configured during personalization phase to operate as Driver Card, Company Card, Workshop Card or Controller Card.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11 February 2021 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]*.

Although this was a new evaluation, the TOE has been previously evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified with the reference CC-19-200716 on 7 January 2019, as reported *[CR-200716]*. This new evaluation was performed as a result of an updated platform used in the composite TOE. 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 IDeal Drive DT V3.1 on Cosmo V9.1, 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 IDeal Drive DT V3.1 on Cosmo V9.1 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 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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 IDeal Drive DT V3.1 on Cosmo V9.1 from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Infineon security controller SLC32GDL400G3 SLC32GDA400G3	IFX_CCI_000005
	Java Card Platform - ID-ONE COSMO V9.1	SAAAAR 092914
Software	IDeal Drive DT v3.1	SAAAAR 416304

To ensure secure usage a set of guidance documents is provided together with the IDeal Drive DT V3.1 on Cosmo V9.1. 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 4.

2.2 Security Policy

The main security features of the TOE are as follows:

a) The TOE must preserve card identification data and user identification data stored during the card personalisation process;

b) The TOE must preserve user data stored in the card by Vehicle Units

c) The TOE must allow certain write operations onto the cards to only an authenticated VU.

Specifically the Tachograph Card aims to protect:

a) The data that is stored in such a way as to prevent unauthorised access to and manipulation of the data, and to detect any such attempts;

b) The integrity and authenticity of data exchanged between the recording equipment and the Tachograph Card.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

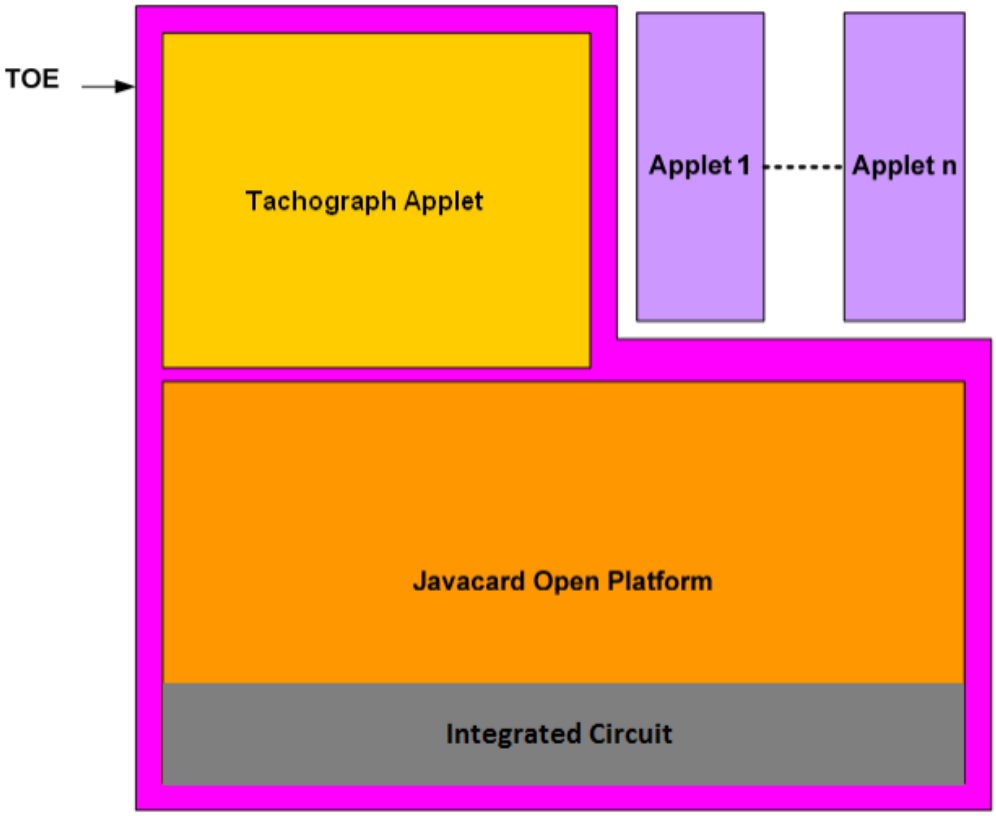
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 6.5 of the *[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.

2.4 Architectural Information

The TOE is an Integrated Circuit and its embedded software, composed of the Tachograph Java Card applet on top of a Java Card Open Platform ID-One Cosmo v9.1. The scope of the TOE is as follows:



The TOE is composed of 3 subsystems, which correspond to the 3 java packages that form the Tachograph applet (2 applets and 1 library) in the implementation representation. Note that the platform is not covered by the TOE design provided by the developer, although it is considered as an additional subsystem supporting the tachograph applet and implementing some specific SFRs as detailed in the Statement of compatibility of *[ST]*.

2.5 Documentation

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

Identifier	Version
IDeal Drive DT v3.1 AGD_OPE, FQR 401 8522	Ed 1
IDeal Drive DT v3.1 AGD_PRE, FQR 401 8521	Ed 1
ID-One Cosmo v9.1 Biometry Applet Security Recommendations, FQR 110 9237	Ed 2
ID-One Cosmo v9.1 Biometry Pre-Perso Guide, FQR 110 9208	Ed 8
ID-One Cosmo v9.1 Biometry Reference Guide, FQR 110 9200	Ed 6
ID-One Cosmo V9.1 Biometry Application Loading Protection Guidance, FQR 110 9238	Ed 1
JCVM_PATCH, FQR 110 8805	Ed 2
Java Card API on ID-One CosmoV9.1 platform, FQR 110 9242	Ed 1
Secure acceptance and delivery of sensitive elements FQR 110 8921	Ed 1

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 extensive testing of TSFIs for Generation 1 and resp. Generation 2 functionalities for all the tachograph types (Driver, Workshop, Control and Company) which covers the expected behaviour defined in *[EU – 2016/799]* and resp. in *[EU – 1360/2002]*.

The test groups for Generation 1 include a generic test plan for all TOE configurations and additionally, a test group for each configuration. Generation 2 includes three test groups used for all configurations. The test configuration depends on the executed test plan, and it covers both Tachograph Generation 1 and Generation 2 as well as the 4 different card types (Driver, Workshop, Control and Company). All groups use the same Test Environment and Tools.

During the NSCIB-CC-200716 evaluation, the evaluator repeated part of the developer tests by witnessing on site, the sample was focused on testing of the most relevant functionality of the Tachograph specification, covering both Tachograph Generation 1 and Generation 2, as well as the 4 types of Tachograph cards (Workshop, Driver, Control and Company cards). The witnessing procedure was not repeated for this evaluation, because the test set-up and strategy have not changed.

For the testing performed by the evaluators, the developer has provided samples.

During both NSCIB-CC-200216 evaluation and this evaluation, the evaluator devised and executed a set of tests aiming to verify a part of the preparatory guidance and the robustness in the TOE. Additionally, the observations during the test witnessing highlighted that a part of one test case was not covered by the test scripts, therefore the evaluator decided to cover this test case as an evaluator independent test.

2.6.2 Independent Penetration Testing

The independent penetration test plan devised during the NSCIB-CC-200716 evaluation was designed based on the evaluator's white box vulnerability analysis, in compliance with the attack methodology *[JIL-AM]* (using v2.2 at the time) for products claiming resistance to attackers with high attack potential (AVA_VAN.5) and the composite evaluation methodology *[JIL-COMP]*.

During this evaluation, the vulnerability was updated to the latest state of the art and considering *[JC-ETRfC]*. As a result an additional penetration test was identified and added to the penetration test plan.

The total test effort expended by the evaluators was 9 weeks. During that test campaign 100% of the total time was spent on side channel testing.

2.6.3 Test Configuration

Developer's testing for this evaluation was performed on the TOE as defined in 2.1. The specific IC version used was SLC32GDA400G3.

The evaluator testing for this evaluation was performed on the TOE as defined in 2.1. The specific IC version used was SLC32GDA400G3. The independent evaluator tests covered all card configurations, i.e., company, control, driver, and workshop cards.

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 strength of the implementation of the cryptographic functionality has been assessed as part of the evaluation of the underlying Java Card Platform, *[JC-ETRfC].*

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”: The TOE uses cryptographic primitives with security level lower than 100 bits, namely two-key TDES, 1024-bit RSA and SHA-1. The usage of such cryptographic primitives is required by the EU regulation *[EU-TACH]* for backward compatibility with 1st Generation tachograph cards. This is compliant with NSCIB Scheme Interpretation *[NSI_08]* since the TOE does not support composition on top of it.

The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

2.7 Re-used evaluation results

This has been performed effectively as a re-certification using NSCIB-CC-200716 as a baseline. 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.

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 IDeal Drive DT V3.1 on Cosmo V9.1, as described in the identification part of this report

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 IDeal Drive DT V3.1 on Cosmo V9.1, to be CC Part 2 extended, CC Part 3 conform**ant**, 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 Profiles *[PP-GEN1]* and *[PP-GEN2].*

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. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. In order to be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The IDeal Drive DT v3.1 on Cosmo V9.1 - Security Target, FQR 550 0044, Ed 1, 20/10/2020 *[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
VU	Vehicle Unit

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-200716]	Certification Report IDeal Drive DT V3.0, NSCIB-CC-200716-CR, v1, 7 January 2019.
[ETR]	Evaluation Technical Report IDeal Drive DT 3.1 on COSMO V9.1, 20-RPT-1299, Version 4.0, 11 February 2021.
[EU-TACH]	[EU – 2016/799] Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components. [EU – 2018/502] Commission Implementing Regulation (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components. [EU – 1360/2002] Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002, Annex 1B, and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71).
[JC-CERT]	Rapport de certification, ANSSI-CC-2020/07, Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32, Identification du matériel 092914, 31/03/2020, including Maintenance Report: Rapport de maintenance, ANSSI-CC-2020/07-M01, Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32, Identification du matériel 092914, 23/07/2020.
[JC-ETRfC]	ETR for composite evaluation – PYRRHA, LETI.CESTI.PYR.RTC.001, V1.1, 12/03/2020.
[JC-ST]	ID-One COSMO v9.1 Public Security Target, FQR 110 9395, version 5, 10/07/2020.
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (controlled distribution).
[JIL-COMP]	Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, Joint Interpretation Library, May 2018.
[JIL-AP]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[NSI_08]	NSCIB Scheme Instruction 08, Performing Testing, Version 2.6, 10 August 2020.
[PP-GEN1]	Common Criteria Protection Profile: Digital Tachograph – Smart card (Tachograph Card), registered under the reference BSI-CC-PP-0070, Version 1.02, 15 November 2011.
[PP-GEN2]	Common Criteria Protection Profile: Digital Tachograph –Tachograph Card (TC PP), registered under the reference BSI-CC-PP-0091, Version 1.0, 9 May 2017.

[ST]	IDeal Drive DT v3.1 on Cosmo V9.1 - Security Target, FQR 550 0044, Ed 1, 20/10/2020.
[ST-lite]	IDeal Drive DT v3.1 on Cosmo V9.1 – Public Security Target, FQR 550 0168, Ed 1, 14/12/2020.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).