

Certification Report

IDEal Drive DT V3.0

Sponsor and developer: **IDEMIA**
Défense Ouest - 420 rue d'Estienne d'Orves
92700 Colombes
France

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

Report number: **NSCIB-CC-200716-CR**
Report version: **1**
Project number: **200716**
Author(s): **NLNCSA/Carolina Lavatelli**
Date: **7 January 2019**
Number of pages: **12**
Number of appendices: **0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Certificate

Standard Common Criteria for Information Technology Security Evaluation (CC),
Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number **CC-19-200716**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder
and developer

IDEMIA

Défense Ouest - 420 rue d'Estienne d'Orves
92700 Colombes, France

Product and
assurance level

IDeal Drive DT V3.0

Assurance Package:

- EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

Protection Profile Conformance:

- Digital Tachograph – Tachograph Card (TC PP), registered under the reference BSI-CC-PP-0091, Version 1.0, 9 May 2017

Project number **200716**

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 EAL 7

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 : **11-01-2019**

Certificate expiry : **11-01-2024**



Accredited by the Dutch
Council for Accreditation

A handwritten signature in blue ink, appearing to be 'C.C.M. van Houten', is written over a horizontal line.

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

CONTENTS:

Foreword	4
Recognition of the certificate	5
International recognition	5
European recognition	5
1 Executive Summary	6
2 Certification Results	7
2.1 Identification of Target of Evaluation	7
2.2 Security Policy	7
2.3 Assumptions and Clarification of Scope	7
2.4 Architectural Information	8
2.5 Documentation	8
2.6 IT Product Testing	8
2.7 Re-used evaluation results	10
2.8 Evaluated Configuration	10
2.9 Results of the Evaluation	10
2.10 Comments/Recommendations	10
3 Security Target	11
4 Definitions	11
5 Bibliography	12

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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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 V3.0. The developer of the IDEal Drive DT V3.0 is IDEMIA located in Colombes, 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.

IDEal Drive DT V3.0 (TOE) is a contact Digital Tachograph card compliant with European regulation [EU-TACH] and Tachograph Protection Profile [PP-TACH]. IDEal Drive DT V3.0 implements Generation 1 and Generation 2 modes and supports the configuration to the following Tachograph card types: Driver card, Workshop card, Control card and Company card. The Tachograph card type is set during the personalization phase. IDEal Drive DT V3.0 provides the following main functionalities:

- Store card and cardholder identification data. This data is used by the Vehicle Unit to identify the cardholder, provide services and data access rights accordingly, and ensure cardholder accountability for his activities.
- Store cardholder activities data, events and faults, and control activities data.

The TOE in the usage phase is composed of the IC and dedicated embedded software, the Java Card system, GlobalPlatform card management component and the Tachograph applet. The TOE can be delivered under different form factors such as wafer, micro-module or smartcard.

This evaluation has been performed as a composite evaluation on IDEMIA ID-ONE Cosmo V9 Essential version 3 (Cosmo V9) Java Card platform on Infineon IFX_CCI_000005, IFX_CCI_000008, IFX_CCI_000014 certified ICs, which has been certified under NSCIB with reference CC-18-200833 [PL-CERT].

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 19th December 2018 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 IDEal Drive DT V3.0, 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 V3.0 are advised to verify that their own environment is consistent with the security target, to apply the recommendations provided in the security guidance [AGD_PRE], [AGD_OPE] and [KEY_MGT], 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 it meets the EAL4 augmented (EAL4(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), ATE_DPT.2 (Testing security enforcing modules) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 [CEM], for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 [CC].

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the IDEal Drive DT V3.0 from IDEMIA located in Colombes, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Infineon security controller	IFX_CCI_000005
		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
	IDEal Drive DT v3.0 (tachograph applet)	SAAAAR 416303

To ensure secure usage a set of guidance documents is provided together with the IDEal Drive DT V3.0. 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-Lite]*, chapter 3.2.

2.2 Security Policy

IDEal Drive DT V3.0 is a contact Tachograph card that implements the EU directive [EU-TACH], which comprises the following main functions:

- Store card and cardholder identification data. This data is used by the Vehicle Unit to identify the cardholder, provide services and data access rights accordingly, and ensure cardholder accountability for his activities.
- Store cardholder activities data, events and faults, and control activities data.

IDEal Drive DT V3.0 supports the configuration to the following Tachograph card types: Driver card, Workshop card, Control card and Company card.

The main security features of the TOE are the following:

- Prevent and detect unauthorised data access or manipulation.
- Enforce integrity and authenticity of the data exchanged with the recording equipment.

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. Details can be found in *[ST-Lite]* section 4.5. 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 5.2 of the *[ST-Lite]*.

2.3.2 Clarification of scope

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

Refer to the certification report NSCIB-CC-200833-CR for clarification of the scope of the evaluation of the underlying Java Card platform.

2.4 Architectural Information

The TOE consists of the Infineon IC, the Java Card Open Platform ID-One Cosmo v9.0 Essential version 3 and the “Tachograph Applet” shown in Figure 2-1. The “Tachograph Applet” is a Java Card package implementing the Tachograph functionality, which is composed of three subsystems: a tachograph personalisation applet that is deleted after personalisation and before entering the usage phase, and the tachograph applet for the usage phase and a supporting library used by these two applets.

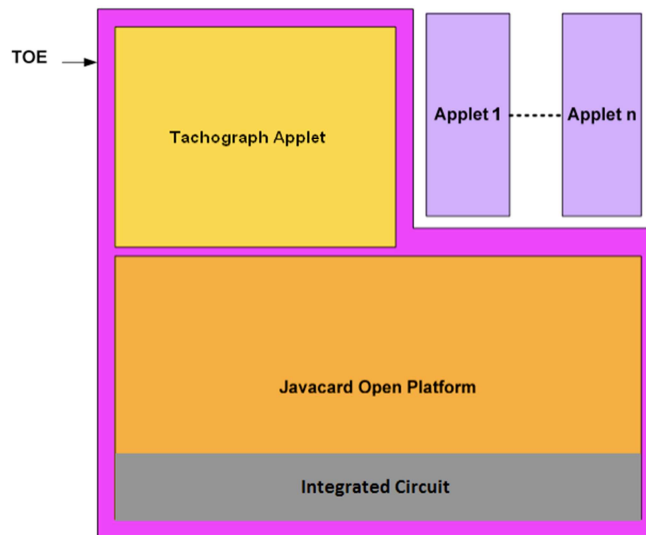


Figure 2-1: TOE scope

2.5 Documentation

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

Identifier	Version
[AGD_OPE] IDEal Drive DT v3.0 AGD_OPE	FQR 401 7909 Ed 3, 15 Nov 2018
[AGD_PRE] IDEal Drive DT v3.0 AGD_PRE	FQR 401 7997 Ed 4, 26 Oct 2018
[KEY_MGT] Key Management Procedure for R&D Centers	I CRD13 2 CRD 510 02

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 Generation 2 functionalities for all the tachograph types (Driver, Workshop, Control and Company) which covers the expected behaviour defined in [EU – 2016/799]. All the APDU commands have been tested for positive/negative cases. The developer has also performed unit testing of the modules' interfaces. The interaction between the TOE's subsystems has been tested using these two sets of tests. The security mechanisms which could not be tested at the interfaces have been verified through code review.

The evaluator has repeated part of the developer tests by witnessing on site, and defined a set of complementary tests of TOE identification, hidden commands, specific access conditions and control flow.

2.6.2 Independent Penetration Testing

The independent penetration test plan has been designed based on the evaluator's white box vulnerability analysis, in compliance with the attack methodology [JIL-AM] for products claiming resistance to attackers with high attack potential (AVA_VAN.5) and the composite evaluation methodology [JIL-COMP].

The vulnerability analysis has followed the two main steps of the method described in [AIS34]:

- Examine sources publicly available.
- Conduct a methodical analysis of TOE evidence including the platform ETR for composition [PL-ETRFc] and the implementation representation.

The vulnerability analysis gave rise to one side-channel penetration test.

2.6.3 Test Configuration

Developer's testing has been performed on the TOE as defined in 2.1 (applet version 416303 on Java Card platform version 089233).

Evaluator's independent and penetration testing has been performed on applet version 416303 on Java Card platform version 089232. The evaluator has analysed the differences between platform versions 089232 and 089233 and concluded that the results are valid for 089233 since the modifications do not impact the security or the behaviour of the TOE.

2.6.4 Testing Results

The testing activities, including the 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 evaluator's independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its [ST] and technical specifications.

No exploitable vulnerabilities were found with the independent penetration tests. No residual vulnerabilities were found.

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 public domain, i.e. from the current best cryptanalytic attacks published, has been considered. The strength of the implementation of the cryptographic functionality has been assessed as part of the evaluation of the underlying Java Card Platform - ID-ONE COSMO V9 ESSENTIAL.

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

There has been extensive re-use of the ALC aspects for the sites involved in the software components of the TOE in France (Colombes, Pessac and Vitré), Indonesia (Jakarta) and China (Shenzen).

The sites involved in the development and production of the IC were re-used by composition through the Java Card platform certificate [PL-CERT].

No site has 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 V3.0, which refers to the hardware and software components identified in section 2.1.

2.9 Results of the Evaluation

The evaluation laboratory documented their evaluation results in the [ETR]², which references the developer evidences.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation laboratory concluded that IDEal Drive DT V3.0 meets the requirements of EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as required in the Security Target [ST], which is strictly conformant with the Protection Profile [PP-TACH].

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”, sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

² The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The Security Target of IDEal Drive DT v3.0, FQR 401 7925 Ed 5 - ST, V1.4, 19 November 2018 [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:

DES	Data Encryption Standard
IC	Integrated Circuit
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
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.
- [ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.
- [JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013 (controlled distribution).
- [JIL-COMP] Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, Joint Interpretation Library, May 2018.
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.
- [NSI_08] NSCIB Scheme Instruction 08, Performing Testing, Version 2.4, 1 June 2018.
- [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).
- [PP-TACH] Digital Tachograph – Tachograph Card (TC PP), registered under the reference BSI-CC-PP-0091, Version 1.0, 9 May 2017.
- [PL-ETRFc] Evaluation Technical Report for Composition ID-ONE Cosmo V9 Essential - EAL5+, 18-RPT-647, Version 5.0, 10 December 2018.
- [PL-CERT] Certification Report ID-ONE Cosmo V9 Essential version 3 (Cosmo V9), NSCIB-CC-200833-CR, Version 1, 11 December 2018.
- [ST] Security Target of IDEal Drive DT v3.0, FQR 401 7925 Ed 5 - ST, V1.4, 19 November 2018.
- [ST-Lite] IDEal Drive DT v3.0 Public Security Target, FQR 550 0007 Ed 1.0, 4 December 2018.
- [AGD_OPE] FQR 401 7909 Ed 3 - IDEal Drive DT v3.0 AGD_OPE, Issue 3, 15 November 2018.
- [AGD_PRE] FQR 401 7997 Ed 4 - IDEal Drive DT v3.0 AGD_PRE, Issue 4, 26 October 2018.
- [KEY_MGT] Key Management Procedure for R&D Centers. Ref: I CRD13 2 CRD 510 02.
- [ETR] Evaluation Technical Report IDEal Drive DT V3.0, 18-RPT-669, Version 7.0, 19 December 2018.

(This is the end of this report).