122

CERTIFICATION REPORT No. CRP272

ID-One Tachograph
Version 1.0

Issue 1.0

December 2012

CESG Certification Body
AAS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme ('the Scheme') and has met the specified Common Criteria (CC) [CC] requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.			
Sponsor:	Oberthur Technologies	Developer:	Oberthur Technologies
Product & Version:	ID-One Tachograph Version 1.0		
Applet:	Tachograph Applet Version 00 00 00 25		
Java Card Open Platform:	ID-One Cosmo v7.0.1-n, as certified in [CR_PLAT].		
Description:	Tachograph Smartcard		
CC Version:	Version 3.1 Release 3		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL4 augmented by AVA_VAN.5, ATE_DPT.2, ALC_DVS.2		
PP Conformance:	Digital Tachograph – Smart Card (Tachograph Card) [PP_TACHO]		
Evaluation Facility:	Underwriters Laboratories (UL) Transaction Security – Commercial Evaluation Facility (CLEF)		
CC Certificate:	P272	Date Certified:	12th December 2012

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE) in meeting its Security Target (ST) [ST] [ST_LITE], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (abbreviated to 'Common Criteria Recognition Arrangement' (CCRA))

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, the CCRA logo which appears below confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and this Certification Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS) MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this report are covered by the CCRA [CCRA] up to EAL4, i.e. the augmentations *AVA_VAN.5*, *ATE_DPT.2* and *ALC_DVS.2* are not covered by the CCRA. All judgements contained in this report are covered by the SOGIS-MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of ID-One Tachograph version 1.0 to the Sponsor, Oberthur Technologies, as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. The Common Criteria Recognition Arrangement [CCRA] requires the Security Target (ST) to be included with the Certification Report. However [CCRA] Appendix I.13 allows the ST to be sanitised by the removal or paraphrasing of proprietary technical information; the resulting document is named ST-lite. For ID-One Tachograph version 1.0, the ST is [ST] and the ST-lite is [ST_LITE].

3. Prospective consumers of ID-One Tachograph version 1.0 should understand the specific scope of the certification by reading this report in conjunction with the ST-lite [ST_LITE], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

4. The following product completed evaluation to CC **EAL4** augmented by AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 on 11th December 2012:

- **ID-One Tachograph version 1.0, comprising Tachograph applet version 00 00 00 25 running on Cosmo v7.0.1-n**

5. The Developer was Oberthur Technologies.

6. The TOE is a Tachograph Smartcard, in accordance with the Commission Regulation (EC) No. 1360/2002 of 13th June 2002 [EU]. It can be personalised as a driver card, workshop card, control card or company card. The TOE is a composite product, composed of the Tachograph applet that is embedded on a previously certified Java Card Open Platform. The Java Card Open Platform has previously been certified by the French Scheme (ANSSI) [CR_PLAT]. Therefore the focus of the composite TOE's evaluation was the Tachograph applet, with the application of Joint Interpretation Library (JIL) guidance for composed smartcard TOEs [JIL_COMP] to consider the underlying Java Card Open Platform.

7. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

8. An overview of the TOE and its product architecture is in Chapter IV 'Product Architecture' of this report. Configuration of the TOE is performed in Phase 6 ('TOE Personalization') of the smartcard lifecycle, as specified in Section 2.3 of [ST].

Protection Profile Conformance

9. The ST [ST] is certified as conformant to the following protection profile:

- Digital Tachograph – Smart Card (Tachograph Card) [PP_TACHO].

10. The ST [ST] also includes objectives and Security Functional Requirements (SFRs) that are additional to those of the protection profile [PP_TACHO].

11. For Phase 6, the ST [ST] adds the following SFRs:

FCS_CKM.1/Perso	FCS_CKM.1/Perso_GP	FCS_CKM.2/Perso	FCS_COP.1/Perso
FDP_ACC.2/Perso	FCS_ACF.1/Perso	FDP_ETC.1/Perso	FDP_ITC.1/Perso
FDP_UCT.1/Perso	FIA_AFL.1/Perso	FIA_ATD.1/Perso	FIA_UAU.1/Perso
FIA_UAU.4/Perso	FIA_UAU.7/Perso	FIA_UID.1/Perso	FMT_MOF.1/Perso
FMT_MTD.1/Perso	FMT_SMF.1/Perso	FMT_SMR.2/Perso	FTP_ITC.1/Perso

12. The ST [ST] also adds the following SFR for Phase 6 and Phase 7 ('TOE Usage'):

- FCS_RNG.1

13. The assurance package *E3hCC31_AP* defined in [PP_TACHO] as EAL4 + AVA_VAN.5, ATE_DPT.2, has been further augmented by ALC_DVS.2 for the TOE.

Security Target

14. The ST [ST] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which those Objectives counter / meet and the Security Functional Requirements (SFRs) that refine the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of that standard facilitates comparison with other evaluated products. The extended requirements *FPT_EMS.1 TOE Emanation* and *FCS_RNG.1 Random Number Generation* are defined in Section 5 of [ST].

15. The TOE security policies are detailed in the ST [ST]. The OSPs that must be met are specified in [ST] Section 3.4.

16. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

17. The TOE is a Javacard Applet embedded in a previously certified Java Card Open Platform, so additional supporting documentation and evidence related to the JIL composite model has been used. The applied documentation is the following:

a) JIL supporting documents for composite product evaluation of smartcard and similar devices: [JIL_COMP] and [JIL_ARC], including Appendix 1.

b) JIL attack methods [JIL_AM] and attack potential [JIL_AP] for smartcards and similar devices.

c) ETR-lite for composition for the Java Card Open Platform [ETR_COMP].

d) Java Card Open Platform documentation provided by the Sponsor to support the composite evaluation: [ST_PLAT], [SR_PLAT], [REF_PLAT] and [PRE_PLAT].

e) Java Card Open Platform certification report [CR_PLAT], issued by ANSSI.

18. The Evaluators' testing of the TOE was performed entirely at the provisionally-appointed Commercial Evaluation Facility of UL Transaction Security ('the CLEF') in Basingstoke, UK. All of the testing was performed on the final TOE, i.e. the Applet embedded on the previously certified Java Card Open Platform.

19. Oberthur Technologies' development and manufacturing sites had previously and separately been assessed in the context of other evaluations at the same assurance level (i.e. EAL4), so the CLEF re-used the evaluation results of Assurance class ALC (i.e. Life-cycle Support) activities relating to those sites. Therefore, as agreed in advance with the CESG Certification Body, no site visits were performed by the CLEF for the evaluation of the TOE.

20. Application Note 10 [NOTE10] has been taken into account in this evaluation. The list of known applets loaded on the previously certified Java Card Open Platform is stated in [APP_PLAT].

21. The CESG Certification Body monitored the evaluation by the CLEF and witnessed a sample of the Evaluators' tests. The evaluation addressed the requirements specified in the ST [ST]. The results of the evaluation, completed in December 2012, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

22. The TOE should be used in accordance with the environmental assumptions specified in the ST [ST] / ST-lite [ST_LITE]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

23. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Conclusions

24. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

Recommendations

25. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

26. In addition, the Evaluators' comments and recommendations are as follows:

- The TOE provides secure Personal Identification Number (PIN) verification services. It is the Vehicle Unit's responsibility to take appropriate actions to ensure the PIN authentication of the cardholder. As such, the Vehicle Unit shall fulfill requirement UIA_212 stated in Commission Regulation (EC) No. 1360/2002 of 13th June 2002: Annex I B, Appendix 11 [EU_11]. The consumer should ensure that this is consistent with the environment in which the TOE is to be deployed.

Disclaimers

27. This Certification Report and associated Certificate apply only to the specific version of the TOE in its evaluated configuration. This is specified in Chapter III 'Evaluated Configuration' of this report. The ETR [ETR] on which this Certification Report is based relates only to the specific item(s) tested.

28. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

29. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V) and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

30. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

31. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

32. Note that the opinions and interpretations stated in this report under 'Recommendations' and 'TOE Security Guidance' are based on the experience of the CESG Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

33. The following sections provide guidance of particular relevance to purchasers of the TOE.

Delivery and Installation

34. On receipt of the TOE, the consumer should check that the evaluated version has been supplied and that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the TOE documents detailed below:

a) Section 6 of [AGD_PRE] describes the actions to be taken by the Personalisation Administration agent upon receipt of the TOE.

b) Section 7 of [AGD_PRE] describes the procedure for identification of the TOE, including Applet and Java Card Open Platform identification. Specific details for the Java Card Open Platform identification are in [CR_PLAT]. Users can identify the TOE with the following procedure:

- Answer to GET DATA (performed under the Applet) with P1P2 = DF67 should be:

```
00 00 00 25
```

identifying the Applet version.

- Answer to GET DATA (performed under the Card Manager) with P1P2 = DF50 returns 20 bytes and the Status Word (SW), for example:

```
00 01 31 43 05 95 45 40 00 38 0B 10
05 41 21 07 44 31 34 31 90 00
```

The bolded byte `0x44` identifies the Integrated Circuit (IC), i.e. P5CD081V1A. Allowed values of this byte are `0x43` (P5CC081V1A) and `0x42` (P5CD041V1A).

- Answer to GET DATA (performed under the Card Manager) with P1P2 = DF52 returns:

```
01 01 1F 02 02 04 50 03 02 18 01 04
06 07 71 21 01 82 0A 05 01 00 06 17
00 2B 00 00 00 FF 00 00 00 00 00 01
00 00 00 00 00 96 FF 69 00 00 00 07
01 0F 08 0B 00 31 C0 64 1F 18 01 00
00 90 00 09 09 41 E8 01 F7 C0 03 CA
E9 F2 90 00
```

The bolded bytes `0x1801` identify the Javacard Open Platform ID-One Cosmo V7.0.1-n. The bolded byte `0x1F` qualifies the Platform as Standard Dual. Other allowed values of that byte are `0x1A` (Standard) and `0x1B` (Basic Dual). The bolded bytes `0x06077121` identify the patch code version 077121.

35. In particular, Users should note that the delivery of the Global Platform keys required for TOE personalisation should be completed in accordance with [KEY_MAN].

Guidance Documentation

36. The Secure Configuration documentation is: [AGD_PRE].

37. The User Guide and Administration Guide documentation is: [AGD_OPE].

III. EVALUATED CONFIGURATION

TOE Identification

38. The TOE is ID-One Tachograph Version 1.0, comprising a Tachograph applet (version 00 00 00 25) running on the certified underlying Java Card Open Platform Cosmo V7.0.1-n masked on the NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) and P5CD041 V1A (Basic Dual) Integrated Circuits (ICs).

TOE Documentation

39. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Guidance Documentation') of this report.

TOE Scope

40. The TOE Scope is defined in the ST [ST] Section 2.1. The TOE lifecycle is summarised in Figure 1 below; the evaluation included Phases 6 and 7 of that lifecycle.

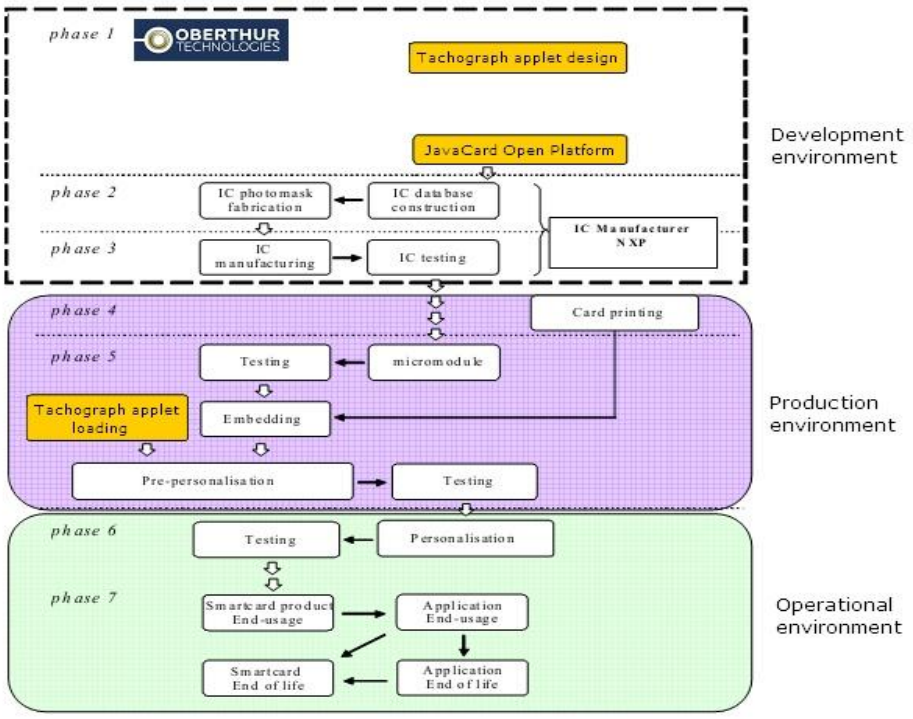

Figure 1 - TOE Lifecycle

TOE Configuration

41. The evaluated configuration of the TOE is defined in the ST [ST] Section 2.1. It includes the 4 configurations of the TOE, i.e. driver card, workshop card, control card and company card.

42. The evaluated configuration considered the NXP P5CD081 V1A IC using the contact interface. The other variants of the IC (i.e. P5CC081 V1A and P5CD041 V1A) provide the same security features; they only differ in the EEPROM size and the support of dual contact/contactless interface, as stated in their Certification Report [CR_IC].

Environmental Requirements

43. The environmental assumptions for the TOE are stated in the ST [ST] Section 3.5.

44. The TOE does not rely on the environment to operate securely, although the environmental IT configuration requires a card reader.

Test Configurations

45. The Developer used the following configuration for their testing:

a) Applet:

- Driver, Workshop, Company and Control cards in Phases 6 and 7;
- Version number 00 00 00 25.

b) Java Card Open Platform: ID-One Cosmo V7.0.1-n Standard Dual.

c) Integrated Circuit: NXP P5CD081 V1A (Standard Dual). Testing was performed using the contact interface.

46. The Evaluators used the same configuration for their testing as that used by the Developer.

IV. PRODUCT ARCHITECTURE

Introduction

47. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

48. The TOE is a composite smartcard product, comprising a Tachograph Applet running on a previously certified Java Card Open Platform.

49. The basic functions of the Tachograph Card are:

a) To store card identification and cardholder identification data. This data is used by the Vehicle Unit to identify the card holder, provide functions and data access rights accordingly, and ensure that the cardholder is accountable for his activities.

b) To store cardholder activities data, events and faults data, and control activities data, related to the cardholder.

50. The main security features of the TOE are as specified in Commission Regulation (EC) No. 1360/2002 of 13th June 2002: Annex I B, Appendix 10 [EU_10]:

a) The TOE must preserve card identification data and cardholder identification data stored during the card personalisation process.

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

51. Specifically, the Tachograph Card aims to:

a) Protect the data stored in such a way as to prevent unauthorised access to and manipulation of the data, and detecting any such attempts.

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

52. The TOE is therefore intended to be used by a card interface device of a Vehicle Unit. It may also be used by any card reader (e.g. of a personal computer) provided that it has the appropriate access rights.

Product Description and Architecture

53. The architecture of the TOE consists of the following elements, as shown in Figure 2:

a) A certified Platform, which includes a Java Card Open Platform masked on a secure chip. The Java Card Open Platform provides a number of security services that are used securely by the Tachograph Applet. The list of security features includes, but is not limited to, the following:

- Secure execution environment, providing effective Applet isolation;
- Card Content Management;
- Global Platform services;
- Secure cryptographic services;
- Secure message digest and signature services;
- Random Number Generation compliant with ANSI X9.31 standard;
- Data integrity and coherency;
- Protection against physical, fault injection and observation attacks.

For a complete list of the security features of the Java Card Open Platform, refer to [ST_PLAT].

b) A Tachograph Java Applet that implements the Tachograph functions and protocols.

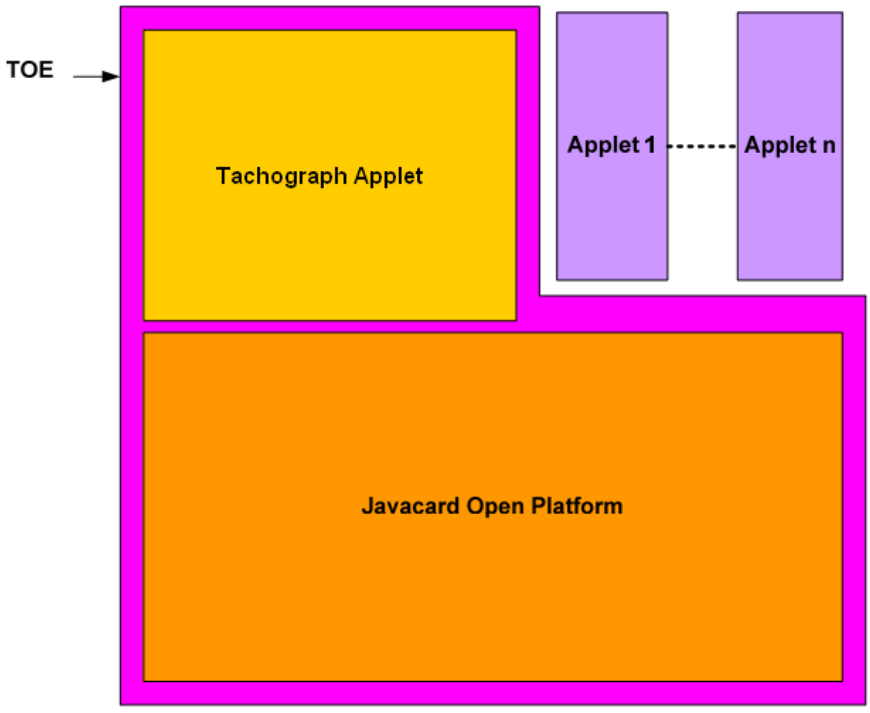

Figure 2 - TOE Architecture

54. The main security features stated above are provided by the following major security services (please refer to [EU_10], Chapter 4):

a) User and Vehicle Unit identification and authentication;

b) Access control to functions and stored data;

c) Accountability of stored data;

d) Audit of events and faults;

e) Accuracy of stored data;

f) Reliability of services;

g) Data exchange with a Vehicle Unit and export of data to a non-Vehicle Unit;

h) Cryptographic support for 'identification and authentication' and 'data exchange' as well as for key generation and distribution in corresponding case according to [EU_11], sec. 4.9.

55. All cryptographic mechanisms including algorithms and the length of corresponding keys have been implemented exactly as required and defined in Commission Regulation (EC) No. 1360/2002 of 13th June 2002: Annex I B, Appendix 10 [EU_10] and Appendix 11 [EU_11].

56. The Security Functions (SFs) provided by the TOE are as follows:

a) Access control in reading;

b) Access control in writing;

c) Authentication during Phase 7;

d) Clearing of sensitive information;

e) Data recording;

f) Errors messages and exceptions;

g) Key management;

h) Signature;

i) Administrator Authentication (Phase 6);

j) Physical protection;

k) Safe state management;

l) Secure messaging;

m) Self-tests.

TOE Design Subsystems

57. The high-level TOE subsystems, and their security features/functionality, are as follows:

a) Javacard Platform subsystem, which represents the Java Card Open Platform.

b) Command manager subsystem, which forms the core of the Tachograph applet. It processes the Application Protocol Data Units (APDUs), implements the mutual authentication protocol and secure channel, provides access control to the filesystem, etc.

c) Key manager subsystem which implements the file system and ensures the integrity of the stored data. It also provides a secure store for loaded certificates into the TOE.

TOE Dependencies

58. The TOE has no dependencies.

TOE Interfaces

59. The external TOE Security Functions Interface (TSFI) is described as follows:

a) APDU commands supported by the TOE in Phase 7 are described in the TOE operational guidance [AGD_OPE].

b) Specific APDU commands related to Global Platform authentication and Card Management for Phase 6 are described in the Platform's reference guide [REF_PLAT] and the TOE's preparative guidance [AGD_PRE].

V. TOE TESTING

Developer Testing

60. The Developer's security tests covered:

a) all SFRs;

b) all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;

c) all SFs;

d) the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

61. The Developer's security tests also included Applet unit testing of the modules and subsystems interfaces. The Evaluators witnessed a video recording of those tests.

Evaluator Testing

62. The Evaluators devised and ran a total of 17 independent security functional tests, different from those performed by the Developer. No anomalies were found.

63. The Evaluators also devised and ran a total of 7 security penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

64. See 'Evaluated Configuration' in this report for a description of the testing configuration.

65. The Evaluators completed their penetration tests on 19th October 2012.

Vulnerability Analysis

66. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on:

a) the visibility of the TOE provided by the evaluation deliverables, particularly the Applet source code;

b) the JIL document 'Attack Methods for Smartcards and Similar Devices' [JIL_AM];

c) the CLEF's knowledge of the latest trends in smartcard attacks, e.g. via its regular participation in the JIL Hardware Attacks Subgroup, smartcard industry conferences, etc.

67. During the vulnerability analysis, a number of potential vulnerabilities were hypothesised and tested later during penetration testing. All potential vulnerabilities identified during the analysis were found to be not exploitable.

Platform Issues

68. No platform issues were identified.

VI. REFERENCES

[AGD_OPE] Tachograph Javacard Applet – AGD_OPE,
Oberthur Technologies,
FQR 110 6217, Issue 2, 4th September 2012.

[AGD_PRE] Tachograph Javacard Applet – AGD_PRE,
Oberthur Technologies,
FQR 110 6325, Edition 1, 12th June 2012.

[APP_PLAT] ID-One Cosmo V7.0.1 – Applications on ID-One Cosmo V7.0.1,
Oberthur Technologies,
FQR 110 6199, Issue 1, 10th April 2012.

[CC] Common Criteria for Information Technology Security Evaluation
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[CR_IC] Certification Report for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and 1P5CD016V1A, each with IC dedicated software,
Bundesamt für Sicherheit in der Informationstechnik,
BSI-DSZ-CC-0555-2009, V1.0, 10th November 2009.

[CR_PLAT] Certification Report ANSSI-CC-2012/30,
Agence nationale de la sécurité des systèmes d'information,
ANSSI-CC-2012/30, 28th September 2012.

[ETR] ID-One Tachograph version 1.0 Evaluation Technical Report,
Underwriters Laboratories (UL) Transaction Security CLEF,
RFI\SEC1\FR86582JD01, Version 1.4, 11th December 2012.

[ETR_COMP] Evaluation Technical Report Lite TERPSICHORE-N2,
Thales-CEACI ITSEF,
TERN2_ETR Lite, Revision 1.0, 9th February 2012.

[EU] Commission Regulation (EC) No. 1360/2002 of 13th June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport:
Annex I B: Requirements for construction, testing, installation and inspection,
Commission of the European Communities,
Official Journal of the European Communities, L 207, 5th August 2002;

and last amended by

Commission Regulation (EC) No. 432/2004 of 5th March 2004 adapting for the eighth time to technical progress Council Regulation (EEC) No. 3821/85 of 20 December 1985 on recording equipment in road transport,
European Union,
Official Journal of the European Union, L 71, 10th March 2004;

and

Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport,
European Union,
Official Journal of the European Union, L 77, 13th March 2004.

[EU_10] Commission Regulation (EC) No. 1360/2002 of 13th June 2002:
Annex I B, Appendix 10 - Generic Security Targets,
Commission of the European Communities,
Official Journal of the European Communities, L 207, 5th August 2002.

[EU_11] Commission Regulation (EC) No. 1360/2002 of 13th June 2002:
Annex I B, Appendix 11 – Common Security Mechanisms,
Commission of the European Communities,
Official Journal of the European Communities, L 207, 5th August 2002.

[JIL_AM] Attack Methods for Smartcards and Similar Devices,
Joint Interpretation Library,
Version 2.3, July 2012.

[JIL_AP] Application of Attack Potential to Smartcards,
Joint Interpretation Library,
Version 2.8, January 2012.

[JIL_ARC] Security Architecture Requirements (ADV_ARC) for Smart Cards and Similar Devices,
Joint Interpretation Library,
Version 2.0, January 2012.

[JIL_COMP] Composite Product Evaluation for Smart Cards and Similar Devices,
Joint Interpretation Library,
Version 1.2, January 2012.

[KEY_MAN] Key Management,
Oberthur Technologies,
FQR 800 0340, Issue 1, 14th March 2012.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8th January 2010 (effective April 2010).

[NOTE10] Certification of "Open" Smart Card Products,
Agence nationale de la sécurité des systèmes d'information,
ANSSI-CCNOTE/10EN.01deW10, Version 0.1, 27th July 2012.

[PP_TACHO] Common Criteria Protection Profile:
Digital Tachograph – Smart Card (Tachograph Card),
Bundesamt für Sicherheit in der Informationstechnik,
BSI-CC-PP-0070, Version 1.02, 15th November 2011.

[PRE_PLAT] ID-One Cosmo V7.0.1 Pre-Perso Guide,
Oberthur Technologies,
FQR 110 4910, Issue 7, 16th February 2012.

[REF_PLAT] ID-One Cosmo V7.0.1 Reference Guide,
Oberthur Technologies,
FQR 110 4911, Issue 4.

[SR_PLAT] ID-One Cosmo V7.0.1 - Security recommendations,
Oberthur Technologies,
FQR 110 4912, Issue 4, 2nd August 2012.

[ST] Calliope Security Target,
Oberthur Technologies,
FQR 110 6186, Issue 3, August 2012.

[ST_LITE] ID-One Tachograph Public Security Target,
Oberthur Technologies,
FQR 110 6350, Edition 3, 3rd December 2012.

[ST_PLAT] TERPSICHORE - ST ID-ONE Cosmo V7.0.1-n on P5CD041V1A, P5CC081V1A and P5CD081V1A Security Target,
Oberthur Technologies,
FQR 110 4933, Issue 5, 16th February 2012.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.3, October 2010.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, LAN); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations and acronyms (e.g. CLEF, CR) covered in [UKSP00].

ANSSI	Agence nationale de la sécurité des systèmes d'information (i.e. the French scheme)
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security (i.e. the German scheme)
EC	European Commission
EEC	European Economic Community
EEPROM	Electrically Erasable Programmable Read-Only Memory
EU	European Union
IC	Integrated Circuit
JHAS	JIL Hardware Attacks Subgroup
JIL	Joint Interpretation Library
PIN	Personal Identification Number
SW	Status Word
UL	Underwriters Laboratories

This page is intentionally blank.