122

MAINTENANCE REPORT MR1
(supplementing Certification Report No. CRP275)

ID-One CIE
Version 1.0
running on SLE77CLFX2400P (M7794) Integrated Circuit

Issue 1.0

March 2015

CESG Certification Body
Industry Enabling Services, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT (ADDENDUM)

Assurance in the product below has been maintained under the UK IT Security Evaluation and Certification Scheme ('the Scheme') and has met the Common Criteria (CC) [CC] requirements. The scope of the maintenance and the assumed usage environment are specified in this Maintenance Report.			
Sponsor:	Oberthur Technologies	Developer:	Oberthur Technologies
Product and Version:	**Original Certified**: ID-One CIE Version 1.0, *comprising Applet 078384 and Javacard platform 081891*, running on the integrated circuit (IC) identified below. **Latest Derived**: ID-One CIE Version 1.0 *comprising Applet 078385 and Javacard platform 081893*, running on the IC identified below.		
Integrated Circuit:	Infineon Technologies SLE77CLFX2400P (M7794) *(CC Certificate BSI-DSZ-CC-0917-2014)*		
Description:	Secure Signature Creation Device (SSCD) Type 2 and Type 3		
CC Version:	Version 3.1 Release 4		
CC Part 2:	Extended	CC Part 3:	Conformant
PP(s) Conformance:	CEN Workshop Agreement (CWA) 14169:2004 Secure signature-creation devices "EAL4+": • Appendix B - Protection Profile - SSCD Type 2, v1.04, EAL 4+, 25 July 2001; and • Appendix C - Protection Profile - SSCD Type 3, v1.05, EAL 4+, 25 July 2001		
EAL:	EAL4 augmented by AVA_VAN.5 and ALC_DVS.2		
Related CC Certificate:	P275		
Date Maintained:	13th March 2015		

The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the maintenance was to allow minor changes (i.e. those shown to have little or no effect on assurance) to the certified Target of Evaluation (TOE) and/or the IT environment and/or the development environment, and to recognise that the latest derived TOE maintains the same assurance as the original certified TOE.

For the latest derived TOE, its Security Target (ST) is [ST1] and prospective consumers should read its ST-lite [ST1_LITE].

The maintenance was performed in accordance with CC Recognition Arrangement (CCRA) supporting document *"Assurance Continuity: CCRA Requirements"* [AC], and UK Scheme Publications 01 [UKSP01] and 03 [UKSP03P1, UKSP03P2].

The issuance of this report and the maintenance addendum is confirmation that the maintenance process was performed properly and that no *exploitable* vulnerabilities were found in the latest derived TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (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, this confirms that this report and the maintenance addendum have been issued by or under the authority of a Party to this Arrangement and is the Party's claim that this report and the maintenance addendum have been issued in accordance with the terms of this Arrangement.

The judgments[1] contained in this report and the maintenance addendum are those of the Qualified Certification Body which issued them. 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 this report and the maintenance addendum have been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that this report and the maintenance addendum have been issued in accordance with the terms of this Agreement.

The judgments[2] contained in this report and the maintenance addendum are those of the compliant Certification Body which issued them. 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 in this report and the maintenance addendum are covered by the CCRA [CCRA] up to EAL4, i.e. the augmentations AVA_VAN.5 and ALC_DVS.2 are not covered by the CCRA.

[2] All judgements in this report and the maintenance addendum are covered by the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. INTRODUCTION

Overview

1. This Maintenance Report [MR1] states the outcome of the Common Criteria (CC) [CC] Assurance Continuity [AC] process for ID-One CIE Version 1.0, comprising Applet 078385 and Javacard platform 081893, running on integrated circuit (IC) SLE77CLFX2400P (M7794), as summarised on page 2 of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their requirements.

2. The baseline for this report was the original CC evaluation of ***ID-One CIE Version 1.0, comprising Applet 078384 and Javacard platform 081891, running on IC SLE77CLFX2400P (M7794)***, which was certified in August 2014 by the CESG Certification Body to CC EAL4 augmented by AVA_VAN.5 and ALC_DVS.2.

3. The CC Recognition Arrangement (CCRA) [CCRA] requires the Security Target (ST) to be included with the Certification Report. However Appendix I.13 of [CCRA] allows the ST to be sanitised by removing or paraphrasing proprietary technical information; the resulting document is named "ST-lite". For the original certified TOE, the ST was [ST] and the ST-lite was [ST_LITE].

4. Prospective consumers are advised to read the following documents, which are available on the CESG website (www.cesg.gov.uk) and the CC website (www.commoncriteriaportal.org):

a) the ST-lite [ST_LITE] for the original certified Target of Evaluation (TOE), and the ST-lite [ST1_LITE] for the latest derived TOE;

b) the Certification Report [CR] for the original certified TOE [CR], and this Maintenance Report [MR1]for the latest derived TOE;

c) the Certificate (contained in [CR]) for the original certified TOE, and the maintenance addendum (on the above websites) for the latest derived TOE.

5. The Developer of the original certified TOE, and the latest derived TOE, is Oberthur Technologies.

Maintained Version(s)

6. The 'original certified version' of the product was:

- **ID-One CIE Version 1.0, *comprising an Applet (identification code 078384) and a Javacard platform (ID-One Cosmo v9-i, identification code 081891)*, running on certified Infineon Technologies IC SLE77CLFX2400P (M7794)**.

7. The 'latest derived version' of the product for which assurance is maintained is:

- **ID-One CIE Version 1.0, *comprising an Applet (identification code 078385) and a Javacard platform (ID-One Cosmo v9-i, identification code 081893)*, running on certified Infineon Technologies IC SLE77CLFX2400P (M7794)**.

8. The maintenance of the latest derived version is described in this report [MR1], which provides a summary of the incremental changes from the previous certified version [CR].

Assurance Continuity Process

9. The CCRA [CCRA] is a basis for the mutual recognition of the results of CC evaluations and certifications. The CC Assurance Continuity process is defined in *"Assurance Continuity: CCRA Requirements"* [AC] and the UK specific aspects are defined in UK Scheme Publication 01 [UKSP01] and 03 [UKSP03P1, UKSP03P2]. That process is based on an Impact Analysis Report (IAR) by the Developer. The IAR is intended to describe all changes made to the product, including changes to previously-evaluated evidence, and to assess the security impact of each change.

10. For the latest derived version, the Developer followed the above process and performed the following re-testing:

- the Developer performed and verified all functional and security tests;
- the Developer's tests covering security-related functions were unchanged;
- as all changes were considered minor, no additional penetration tests were performed.

11. The Developer produced the IAR [IAR1]. The CESG Certification Body examined [IAR1] and the supporting evidence, then produced this report [MR1] and the maintenance addendum on the CESG website and the CC website.

General Points

12. Assurance Continuity addresses the security functionality claimed, with reference to the assumed environment specified, in the ST/ST-lite. For the latest derived version, its scope, configuration and platform environment are summarised in Chapter II of this report [MR1], in conjunction with the original Certification Report [CR]. Prospective consumers are advised to check that this matches their requirements.

II. ASSURANCE MAINTENANCE

Analysis of Changes

13. [IAR1] is the IAR from the original certified version to the latest derived version, and provides the Assurance Continuity rationale for the latest derived version on the stated platform. [IAR1] conforms to the requirements of [AC] and the UK specific aspects in [UKSP01], [UKSP03P1] and [UKSP03P2].

14. No *Major* changes that could cause a security impact on the TOE were made between the original certified version and the latest derived version. As noted in Chapters 2 and 3 of the IAR [IAR1], all changes were functional changes that did not impact the TOE's security functionality.

15. The changes and their impact on the evaluation deliverables are described in Chapter 2 of [IAR1], which shows that for all changes:

a) The impact of change is determined to be *Minor* or *None*.

b) The effect on the previously-evaluated evidence is determined to be *Minor* or *None*.

c) The action required for resolution is determined to be *None*, as the previously-evaluated evidence has already been updated where appropriate.

Changes to Developer Evidence

16. Section 2.4 of the IAR [IAR1] states that the previously-evaluated evidence that were updated for the latest derived version were as follows:

- Security Target [ST1];
- Public Security Target (i.e. ST-lite) [ST1_LITE];
- Assurance Guidance Document - Preparative Guidance (AGD PRE):
  - Platform AGD PRE [COSMOv9i_PRE1];
  - URANIE AGD PRE [AGD_PRE1];
- Product Generation Description (PGD):
  - Platform PGD [COSMOv9i_PGD1];
  - Applet PGD [PGD1].

17. In addition, discussions between the CESG Certification Body and the Developer [REVIEW1] identified that the following previously-evaluated evidence had been updated for the latest derived version:

- Configuration List [CL1].

18. All updates in the above documents were classified as *Minor* or *None*.

TOE Identification

19. The latest derived version is uniquely identified in Paragraph 7 of this report.

TOE Scope and TOE Configuration

20. The TOE scope is defined in Section 2.1 of the ST-lite [ST1_LITE].

21. The TOE is the whole product. There is only one possible configuration. Hence the TOE configuration is the product configuration.

TOE Documentation

22. Of the Installation, Configuration and Guidance documents listed in the Certification Report for the original certified version [CR], the following have changed for the latest derived version:

- Platform AGD PRE [COSMOv9i_PRE1];
- URANIE AGD PRE [AGD_PRE1].

TOE Environment

23. The TOE environment is defined in Chapter 2 and Section 4.8 of the ST-lite [ST1_LITE].

III. TOE TESTING

Vulnerability Analysis

24. To assess whether any vulnerabilities had been introduced into the TOE between the original certified version and the latest derived version, the Developer's internal security team reviewed vulnerabilities published by relevant sources. Those reviews revealed no new vulnerabilities impacting the TOE and its subsystems.

25. In accordance with the requirements of EAL4 augmented by AVA_VAN.5 and ALC_DVS.2, the Developer performed the same level of vulnerability analysis for the latest derived version as was performed for the original evaluation. The assessed information also contained details of generic vulnerabilities, so any generic vulnerabilities relevant to the TOE were automatically included in the analysis.

26. Chapter 2 of the IAR [IAR1] describes the changes for the latest derived version.

27. During the evaluation of the original version [ETR], the evaluators' vulnerability analysis was based on the Joint Interpretation Library (JIL) *"Attack Methods for Smartcard and Similar Devices"* [JIL_AM] and a search for other public vulnerabilities. For the latest derived version, the Developer repeated that search; no vulnerabilities were found.

28. The CESG Certification Body's review of the IAR [IAR1] and the changes to the previously-evaluated evidence (listed in Paragraphs 16 and 17 of this report), and the Developer's replies, are documented in [REVIEW1]. Those replies confirmed the Developer's search for vulnerabilities, to assess whether any vulnerabilities had been introduced into the TOE between the original certified version and the latest derived version.

29. In summary, no vulnerabilities were found between the original certified version and the latest derived version.

Testing

30. As noted in the CESG Certification Body's review and the Developer's replies [REVIEW1], the Developer performed re-testing of the latest derived version as follows:

- the Developer performed and verified all functional and security tests;
- the Developer's tests covering security-related functions were unchanged;
- as all changes were considered minor, no additional penetration tests were performed.

31. Those tests are listed in Chapter 5 of the Configuration List [CL1].

32. The Developer's test scripts, which had been examined by the Evaluators during the original evaluation [ETR] were appropriately updated for the latest derived version of the TOE. The tests themselves have not changed significantly and they test exactly the same security functionality in the same manner. The Developer holds those updated test scripts.

33. The Developer holds a copy of the original evaluation's Evaluation Test Report [ETR]. The Developer does not hold the Evaluators' test scripts and does not update them.

34. The tests for the latest derived version were run on the platform identified in Paragraph 7 of this report. All of those tests passed and the results did not reveal any inconsistencies or concerns.

35. Thus confidence is established that the latest derived version provides the claimed security functionality in the same manner as the original certified version.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

36. The analysis in the IAR [IAR1] shows that no major changes have been made to the TOE between the original certified version and the latest derived version.

37. The only changes have been categorised as having a ***Minor*** impact and hence EAL4 augmented by AVA_VAN.5 and ALC_DVS.2 assurance has been maintained.

Conclusions

38. The CESG Certification Body accepts the analysis in the IAR [IAR1], which assessed each change as being of ***Minor*** impact, and concludes that the overall impact of all the changes is ***Minor***.

39. The CESG Certification Body has therefore determined that EAL4 augmented by AVA_VAN.5 and ALC_DVS.2, as outlined in the Certification Report [CR], has been maintained for the latest derived version. These conclusions are summarised in the 'Certification Statement (Addendum)' on Page 2 of this report.

40. Prospective consumers of the latest derived version should understand the scope of the maintenance by reading this report in conjunction with the ST-lite [ST1_LITE]. The TOE should be used in accordance with the environmental assumptions specified in [ST1_LITE]. Prospective consumers should check that the Security Functional Requirements (SFRs) and the certified configuration (as maintained for the latest derived version) match their requirements, and should give due consideration to the recommendations and caveats of this report.

41. The TOE should be used in accordance with the supporting guidance in the certified configuration, maintained for the latest derived version. Recommendations on the secure receipt, installation, configuration and operation of the TOE are included in the Certification Report [CR].

Disclaimers

42. The Assurance Continuity process is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered afterwards. This report reflects the CESG Certification Body's views on the date of this report.

43. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the vendor to see if any patches exist for the product and whether those patches have further assurance.

44. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. 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.

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

V. REFERENCES

Common Criteria Documents

[AC] Assurance Continuity: CCRA Requirements,
Common Criteria Development Board,
2012-06-01, Version 2.1, June 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-2012-09-001, Version 3.1 R4, September 2012.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2012-09-002, Version 3.1 R4, September 2012.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2012-09-003, Version 3.1 R4, September 2012.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
2nd July 2014.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2012-09-004, Version 3.1 R4, September 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).

UK IT Security Evaluation and Certification Scheme Documents

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.8, August 2013.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.6, August 2014.

[UKSP03P1] Sponsor's Guide - General Introduction,
UK IT Security Evaluation and Certification Scheme,
UKSP 03 Part I, Issue 3.1, August 2013.

[UKSP03P2] Sponsor's Guide - Assurance Continuity,
UK IT Security Evaluation and Certification Scheme,
UKSP 03 Part II, Issue 1.3, August 2014.

Evaluated Version (Original)

[AGD_PRE] URANIE - AGD PRE,
Oberthur Technologies,
FQR 110 6889, Issue 2, 6th May 2014.

[COSMOv9i_PRE] ID-One Cosmo v9-i platform AGD PRE,
Oberthur Technologies,
FQR 110 7075, Issue 2, 2nd July 2014.

[CR] Common Criteria Certification Report No. CRP275:
ID-One CIE Version 1.0,
CESG Certification Body,
Issue 1.1, August 2014.

[ETR] Evaluation Technical Report,
UL Transaction Security CLEF,
LFU/T006/ETR, Issue 1.2, 27th August 2014.

[JIL_AM] Attack Methods for Smartcards and Similar Devices,
Joint Interpretation Library,
Version 2.2, January 2013.

[ST] URANIE - Security Target - ID-One™ CIE v1.0,
Oberthur Technologies,
FQR 110 6886, Edition 4, 6th August 2014.

[ST_LITE] Public Security Target - ID-One™ CIE Java Applet,
Oberthur Technologies,
FQR 110 7121, Edition 2, undated.

First Derived Version

[AGD_PRE1] URANIE - AGD PRE,
Oberthur Technologies,
FQR 110 6889, Issue 4, 4th February 2015.

[CL1] URANIE - Configuration List,
Oberthur Technologies,
FQR 110 7070, Issue 3, 12th March 2015.

[COSMOv9i_PGD1] ID-One Cosmo v9-i Platform - Product Generation Description (PGD),
Oberthur Technologies,
081893 00 PGD, Issue 3-AA, 28th January 2015.

[COSMOv9i_PRE1] ID-One Cosmo v9-i Platform - AGD PRE,
Oberthur Technologies,
FQR 110 7075, Issue 4, 4th February 2015.

[IAR1] URANIE - Impact Analysis Report,
Oberthur Technologies,
FQR 110 7296, Edition 2, 4th February 2015.

[MR1] Common Criteria Maintenance Report No. CRP275 MR1
(i.e. this document).

[PGD1] ID-One CIE Java Applet - Product Generation Description (PGD),
Oberthur Technologies,
078385 00 PGD, Issue 5-AA, 28th January 2015.

[REVIEW1] CESG Certification Body Review Form for [AGD-PRE1], [CL1], [COSMOv9i_PGD1], [COSMOv9i_PRE1], [IAR1], [PGD1], [ST1] and [ST1_LITE], and Oberthur Technologies Replies, 6th - 13th March 2015.

[ST1] URANIE - Security Target - ID-One™ CIE v1.0,
Oberthur Technologies,
FQR 110 6886, Edition 6, 6th February 2015.

[ST1_LITE] Public Security Target - ID-One™ CIE Java Applet,
Oberthur Technologies,
FQR 110 7121, Edition 4, undated.

VI. ABBREVIATIONS

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

AGD PRE	Assurance Guidance Document - Preparative Guidance
CEN	Comité Européen de Normalisation (European Committee for Standardisation)
CIE	Carta d'Identita Elettronica
CLEF	Commercial Evaluation Facility
CWA	CEN Workshop Agreement
IAR	Impact Analysis Report
IC	Integrated Circuit
MR	Maintenance Report
PGD	Product Generation Description
SSCD	Secure Signature Creation Device