122

CERTIFICATION REPORT No. CRP275

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

Issue 1.1

August 2014

© Crown Copyright 2014 – All Rights Reserved

Reproduction is authorised, provided
this report is copied in its entirety.

CESG Certification Body
Industry Enabling Services, 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 requirements of the Common Criteria (CC) [CC]. The scope of the evaluation and the assumed usage environment are specified in this Certification Report.

Sponsor:	Oberthur Technologies	Developer:	Oberthur Technologies
Product and Version:	ID-One CIE, Version 1.0		
Integrated Circuit:	SLE77CLFX2400P (M7794) *(CC Certificate/Certification Report 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		
CLEF:	UL Transaction Security		
CC Certificate:	P275	Date Certified:	28 August 2014

The evaluation was performed in accordance with the requirements of the 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 the Protection Profiles (PPs) and supporting documents, CC [CC] Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology (CEM) [CEM] and relevant Interpretations.

The issue 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 (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 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 in 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 carried out 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 SOGIS MRA [MRA]. All judgements contained in this report 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.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) [CC] security evaluation of ID-One CIE 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 CIE Version 1.0, the ST is [ST] and the ST-lite is [ST_LITE].

3. Prospective consumers of ID-One CIE 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 in August 2014 to CC Evaluation Assurance Level (EAL) EAL4 augmented by AVA_VAN.5 and ALC_DVS.2:

- **ID-One CIE Version 1.0, running on SLE77CLFX2400P (M7794)**.

5. The Developer was Oberthur Technologies.

6. The evaluated configuration of the product is described in this report as the Target of Evaluation (TOE). For this product, the TOE is the whole product, hence has only one possible configuration (i.e. evaluated configuration = TOE configuration = product configuration).

7. The TOE is a Secure Signature Creation Device (SSCD) Type 2 (key import) and Type 3 (on-card key generation) smartcard product. The TOE is intended to be used as a SSCD Type 2 or Type 3, as defined in Directive 1999/93/EC of the European Parliament and the Council on a Community framework for electronic signatures ("Directive 1999/93/EC") [DIR_EC].

8. Details of the TOE's scope, configuration and environment are provided in Chapter III 'Evaluated Configuration' of this report.

9. An overview of the TOE's architecture is provided in Chapter IV 'Product Architecture' of this report.

Protection Profile Conformance

10. The ST [ST] / ST-lite [ST_LITE] achieved conformance to the following Protection Profiles (PPs):

- Secure Signature Creation Device Type 2 [SSCD2];
- Secure Signature Creation Device Type 3 [SSCD3].

Security Target

11. The ST [ST] / ST-lite [ST_LITE] fully specifies the Assumptions, the Threats, the Security Objectives, the Organisational Security Policies (OSPs) and the Security Functional Requirements (SFRs), for the TOE.

12. Most of the SFRs in the ST [ST] / ST-lite [ST_LITE] are taken from the PPs ([SSCD2], [SSCD3]), which facilitates comparison with other evaluated products.

13. The ST [ST] / ST-lite [ST_LITE] also includes Complementary Assumptions, Complementary Threats, Complementary OSPs, Complementary Security Objectives of the TOE, Complementary Security Objectives of the Environment, Extended Requirements, and Additional SFRs, that are additional to those of the PPs.

Evaluation Conduct

14. The methodology described in the Common Evaluation Methodology (CEM) [CEM] was used to conduct the evaluation. As the TOE is a Smartcard product type, the following supporting documents from the Joint Interpretation Library (JIL) were also used:

- Composite product evaluation for Smart Cards and similar devices [JIL_COMP];
- Application of Attack Methods to Smartcards [JIL_AM];
- Application of Attack Potential to Smartcards [JIL_AP];
- Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices [JIL_ARC].

15. The CESG Certification Body monitored the evaluation, which was performed by the *UL Transaction Security* Commercial Evaluation Facility (CLEF).

16. The Evaluators' testing of the TOE was performed entirely at UL's premises in Basingstoke, UK, using final samples.

17. As agreed in advance with the CESG Certification Body, the evaluation did not perform a site visit, as it re-used the site visit results of a previous evaluation (under the French Scheme).

18. The evaluation addressed the requirements specified in the ST [ST] / ST-lite [ST_LITE]. The results of the evaluation, completed in August 2014, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

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

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

Conclusions

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

Recommendations

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

23. In addition, the Evaluators' recommendation is as follows:

- In accordance with the TOE environment objective *OE.TOE_Construction*, as specified in the ST [ST] / ST-lite [ST_LITE], the Administrator in the Personalisation phase must use due diligence to configure the TOE by correctly following the guidance in "URANIE - AGD PRE" (i.e. Preparative Procedures) [AGD_PRE].

Disclaimers

24. This Certification Report (and associated Certificate) applies only to the specific version of the product in its evaluated configuration (i.e. the TOE). 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.

25. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed on the date stated in paragraph 54 of this report. This report reflects the CESG Certification Body's view on that date.

26. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since that date and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

27. 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.

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

29. Note that the opinions and interpretations stated above in ‘Recommendations’ and in Chapter II ‘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

30. The following sections provide guidance of particular relevance to consumers of the TOE.

Delivery and Installation

31. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the following document:

- "URANIE - AGD PRE" (i.e. Preparative Procedures) [AGD_PRE] Section 5 describes the procedures for identification of the TOE.

32. In particular, Users and Administrators should note that the delivery of the Administrator keys required for TOE personalisation should be completed in accordance with "Key Management" [KEY_MAN].

Guidance Documents

33. The Guidance Documents for the TOE are as follows:

- "URANIE - AGD PRE" (i.e. Preparative Procedures) [AGD_PRE];
- "URANIE - AGD OPE" (i.e. Operational User Guidance) [AGD_OPE].

34. Supporting guidance for the Cosmo v9-i Javacard platform is provided in

- "ID-One Cosmo v9-i Platform AGD PRE" (i.e. Preparative Procedures) [COSMOv9i_PRE];
- "ID-One Cosmo v9-i Platform AGD OPE" (i.e. Operational User Guidance) [COSMOv9i_OPE].

III. EVALUATED CONFIGURATION

TOE Identification

35. The TOE is ID-One CIE Version 1.0, which consists of an Applet (identification code 078384) and a Javacard platform (ID-One Cosmo v9-i, identification code 081891), running on a previously-certified Integrated Circuit (IC) (SLE77CLFX2400P (M7794)) from Infineon Technologies [CR].

TOE Documents

36. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in 'Guidance Documents') of this report.

TOE Scope

37. The TOE Scope is defined in Section 2.1 of the ST [ST] / ST-lite [ST_LITE]. The TOE is delivered at the end of phase 5, so personalisation (phase 6) and final usage (phase 7) occur after delivery.

TOE Configuration

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

Environmental Requirements

39. The TOE does not rely on the environment to operate securely.

40. In accordance with the TOE's environment objective *OE.TOE_Construction* specified in the ST [ST] / ST-lite [ST_LITE], as noted in Paragraph 23 above:

- The Administrator in charge of administrating the TOE in phase 6 shall be a trusted person and shall be skilled enough to correctly apply the recommendations indicated in [AGD_PRE]. These recommendations are required to construct the TOE.

Test Configurations

41. There is only one possible configuration, as indicated in paragraph 38 above. Hence:

- the Developers used that configuration for their testing; and
- the Evaluators used that configuration for their testing.

IV. PRODUCT ARCHITECTURE

Introduction

42. 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.

43. The TOE is a SSCD Type 2 (key import) and Type 3 (on-card key generation) smartcard product developed by Oberthur Technologies. The TOE is intended to be used as a SSCD Type 2 or Type 3, as defined in Directive 1999/93/EC [DIR_EC]. The TOE allows:

- Perform personalisation by an authorised Administrator only in phase 6.
- Perform basic, advanced and qualified signature using RSA and RSA-CRT.
- Authenticate the cardholder based on a PIN. The PIN can be unblocked by the Administrator role in phase 7.
- Authenticate one (or several) administrator(s) of the TOE, that may have special rights to administer the Signature Creation Data (SCD) and Signature Verification Data (SVD) (generation, import), using TDES, RSA or PIN.
- Establish a trusted channel, protected in integrity, confidentiality and authenticity, with remote entities such as a Signature Creation Application (SCA), a Certificate Generation Application (CGA) or a SSCD type 1.
- SCD/SVD pairs and other cryptographic objects may be generated and/or imported after issuance at any time, and in particular, they may be updated during the TOE life cycle

Product Description and Architecture

44. The architecture of the TOE consists of the following elements, as shown in Figure 1.

45. The TOE is a composite product, comprising the CIE Applet running on the Cosmo v9-i Javacard Platform, in composition with the previously-certified M7794 IC from Infineon Technologies [CR]. The Applet and the Javacard Platform have been developed by Oberthur Technologies.

46. The TOE is delivered after phase 5 in closed configuration, meaning that no applets can be loaded.

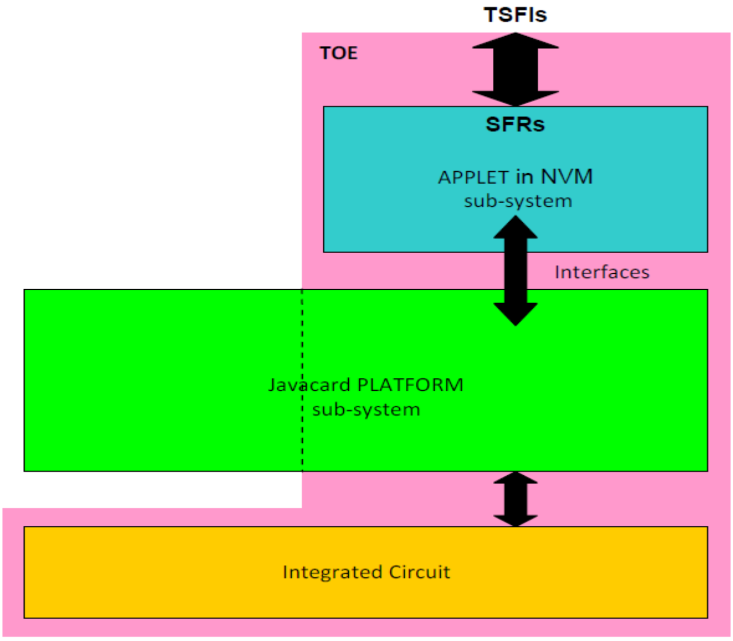

Figure 1: TOE architecture

TOE Design Subsystems

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

- Previously-certified Secure Microcontroller [CR].
- Javacard Platform, which provides a secure execution environment for the Applet, including the Card Manager, the Cryptographic library, the Virtual Machine, the low-level code interfacing with the IC, etc.
- Command Manager, which provides the core functionality of the applet and support for all the commands available. This subsystem is also responsible for implementing the wrapping and unwrapping of secure commands.
- File System, which implements the file system to support the file tree and the Base Security Objects (BSOs).

TOE Dependencies

48. The TOE has no dependencies.

TOE Security Functionality Interface

49. The external TOE Security Functionality Interface (TSFI) is described as follows:

- Application Protocol Data Unit (APDU) commands supported by the TOE in phases 6 and 7 are described in the TOE operational guidance identified in Chapter II (in ‘Guidance Documents’) of this report.

V. TOE TESTING

Developer Testing

50. The Developer's security tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Security Functionality Interface') of this report.

51. The Developer's security tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. The Evaluators witnessed a recording of the execution of those tests.

52. The Developer tested the APDU in the Applet directly. Internal functionality of the Javacard Platform was tested with the Javacard Technology Compatibility Kit (TCK) test suite and with the use of an emulator.

Evaluator Testing

53. The Evaluators devised and ran a total of 4 independent security functional tests, different from those performed by the Developer. No anomalies were found.

54. The Evaluators also devised and ran a total of 11 security penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected. The Evaluators completed their penetration tests on 20th June 2014.

Vulnerability Analysis

55. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in the ETR [ETR], was based on the "JIL Attack Methods for Smartcards and Similar Devices" [JIL_AM] and the visibility of the TOE provided by the evaluation deliverables, in particular the source code of the Applet.

56. Potential vulnerabilities were hypothesised (during the vulnerability analysis) and then tested (during the penetration testing).

57. All potential vulnerabilities identified during the analysis were found to be not exploitable.

Platform Issues

58. The TOE is a smartcard and does not require a platform in its environment. Hence there are no platform issues that should be considered.

VI. REFERENCES

[AGD_OPE] URANIE - AGD OPE,
Oberthur Technologies,
FQR 110 6888, Issue 2.

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

[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,
May 2000.

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

[COSMOv9i_OPE] ID-One Cosmo v9-i platform AGD OPE,
Oberthur Technologies,
FQR 110 7083, Issue 2.

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

[CR] (Certificate/Certification Report): Infineon Technologies Security Controller M7794 A12 and G12 with optional RSA2048/4096 v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software,
Bundesamt für Sicherheit in der Informationstechnik (BSI),
BSI-DSZ-CC-0917-2014, 3rd February 2014.

[DIR_EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,
Official Journal of the European Communities,
L 13, 19 January 2000.

[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.

[JIL_AP] Application of Attack Potential to Smartcards,
Joint Interpretation Library,
Version 2.9, January 2013.

[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).

[SSCD2] Protection Profile – Secure Signature Creation Device Type 2,
CEN Workshop Agreement (CWA) 14169:2004 Appendix B,
Version 1.04, July 2001.

[SSCD3] Protection Profile – Secure Signature Creation Device Type 3,
CEN Workshop Agreement (CWA) 14169:2004 Appendix C,
Version 1.05, July 2001.

[ST] 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 v1.0,
Oberthur Technologies,
FQR 110 7121, Edition 2.

[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 6.5, August 2013.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.5, August 2013.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.8, August 2013.

VII. ABBREVIATIONS

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

APDU	Application Protocol Data Unit
BSO	Base Security Object
CEN	Comité Européen de Normalisation (European Committee for Standardisation)
CGA	Certificate Generation Application
CIE	Carta d'Identita Elettronica
CLEF	Commercial Evaluation Facility
CWA	CEN Workshop Agreement
DES	Data Encryption Standard
IC	Integrated Circuit
JIL	Joint Interpretation Library
PIN	Personal Identification Number
SCA	Signature Creation Application
SCD	Signature Creation Data
SSCD	Secure Signature Creation Device
SVD	Signature Verification Data
TCK	Technology Compatibility Kit
TDES	Triple DES

This page is intentionally blank.

VIII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG

CESG CERTIFICATION BODY

CERTIFICATE No.
P275

This Certificate confirms that

ID-One CIE, Version 1.0

running on SLE77CLFX2400P (M7794) Integrated Circuit

has been evaluated under the terms of the

UK IT Security Evaluation and Certification Scheme

and complies with the requirements for

EAL4 augmented by AVA_VAN.5 and ALC_DVS.2

COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

and the following Protection Profiles:

CWA 14169:2004 Appendix B, Secure Signature Creation Device Type 2 v1.04

CWA 14169:2004 Appendix C, Secure Signature Creation Device Type 3 v1.05

The scope of the evaluated functionality was as claimed by the Security Target
and as confirmed by the associated Certification Report **CRP275**.

Certification is not a guarantee of freedom from security vulnerabilities. This certificate reflects the CESG Certification Body's view at the time of certification. It is the responsibility of users (existing and prospective) to check whether any security vulnerabilities have been discovered since the date of the Evaluators' final penetration tests.

Evaluated and Certified under the UK ITSEC Scheme
UK ITsec

ASSURED PRODUCTS
CESG IACS
ASSURED SYSTEMS

Common Criteria ®

SOGIS
IT SECURITY CERTIFIED

UKAS
PRODUCT CERTIFICATION

AUTHORISATION
Director for Information Assurance

DATE
28 August 2014

122

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ***EN 45011:1998 (ISO/IEC Guide 65:1996)*** to provide product conformity certification as follows:

Category: Type Testing Product Certification of IT Products and Systems.

Standards:
- Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7; and
- Information Technology Security Evaluation Criteria (ITSEC) E1 - E6.

Details are provided on the UKAS website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), May 2000

The CESG Certification Body is a Participant to the above Arrangement. The current Participants to the above Arrangement are detailed on the Common Criteria Portal (www.commoncriteriaportal.org). The mark (left) confirms that this Common Criteria certificate has been authorised by a Participant to the above Arrangement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Arrangement. Upon receipt of this Common Criteria certificate, the vendor(s) may use the mark in conjunction with advertising, marketing and sales of the IT product for which this certificate is issued.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the Arrangement up to EAL4, i.e. the augmentations AVA_VAN.5 and ALC_DVS.2 are not covered by the above Arrangement.

Senior Officials Group – Information Systems Security (SOGIS)

Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgments contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the mark 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.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the above Agreement.

The IT product identified in this certificate has been evaluated by the ***UL Transaction Security*** Commercial Evaluation Facility (an accredited and approved Evaluation Facility of the UK) using the ***Common Methodology for Information Technology Security Evaluation***, ***Version 3.1***, for conformance to the ***Common Criteria for Information Technology Security Evaluation, Version 3.1***. This certificate applies only to the specific version and release of the IT product in its evaluated configuration and in conjunction with the complete, associated Certification Report. The evaluation has been conducted in accordance with the provisions of the UK IT Security Evaluation and Certification Scheme, 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 CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CESG or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

In conformance with the requirements of ***EN 45011:1998 (ISO/IEC Guide 65:1996)***, the ***CCRA*** and the ***SOGIS MRA***, the CESG Certification Body's website (www.cesg.gov.uk) provides additional information, as follows:

- type of product (i.e. product category); and
- details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).

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