122

CERTIFICATION REPORT No. CRP289

ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0

running on SLE77CLFX2400P & SLE77CLFX2407P

Issue 1.0

September 2015

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 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(s), Version(s)	ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0		
Integrated Circuit	Infineon M7794 (SLE77CLFX2400P / SLE77CLFX2407P) Certificate: BSI-DSZ-CC-0917-2014		
Description	Machine Readable Travel Document (MRTD)		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(S) Conformance	Machine Readable Travel Document with "ICAO Application" Extended Access Control [PP]		
EAL or [c]PP	EAL4 augmented by ALC_DVS.2 and AVA_VAN.5		
CLEF	UL Transaction Security		
CC Certificate	P289	Date Certified	7 September 2015

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], 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 [PP] and supporting document [JIL], CC Parts 1, 2 and 3 [CC], 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 (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 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 Certification Report are covered by the CCRA [CCRA] and the SOGIS MRA up to EAL4. The augmentations ALC_DVS.2 and AVA_VAN.5 are not covered by the CCRA but are covered by the SOGIS MRA.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of ePass ICAO essential – configuration BAC and EAC RSA, 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 Oberthur Technologies ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0, the ST is [ST] and the ST-Lite is [ST-Lite].

3. Prospective consumers of ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]/[ST-Lite], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

4. The following product completed evaluation to CC EAL4 assurance level augmented by ALC_DVS.2 and AVA_VAN.5 on [Day] June 2015:

- **ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0 running on SLE77CLFX2400P / SLE77CLFX2407P**

5. The Developer was Oberthur Technologies.

6. The TOE is a Machine Readable Travel Document (MRTD); a multi-applicative native software embedding ICAO application running on Infineon SLE77CLFX2400P and SLE77CLFX2407P Microcontroller.

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. Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

9. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report.

Protection Profile Conformance

10. The Security Target [ST]/[ST-Lite] is certified as achieving conformance to the following Protection Profile:

- Machine Readable Travel Document with "ICAO Application", Extended Access Control [PP].

11. The Security Target [ST]/[ST-Lite] also includes Objectives and Security Functional Requirements (SFRs) additional to those of the Protection Profile.

Security Target

12. The Security Target [ST]/[ST-Lite] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter, the Organisational Security Policies (OSPs) which these Objectives meet and the Security Functional Requirements (SFRs) that refine the Objectives.

13. All of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

14. All threats to the TOE are countered.

15. The TOE security policies are detailed in [ST]/[ST-Lite].

16. The OSPs that must be met are specified in [ST]/[ST-Lite] Section 6.4.

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

18. The cryptographic algorithms are specified in [ST]/[ST-Lite] Section 1.1.

Evaluation Conduct

19. The methodology described in [CEM] has been used to conduct the evaluation, together with interpretations [AIS31] and [AIS34]. The TOE is a smart card product type, so additional supporting documentation related to the Joint Interpretation Library (JIL) has been used. The applied documentation is the following:

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

20. The application source code has been reviewed in Oberthur premises in Colombes, France. Code review for the cryptographic library was also performed in Oberthur premises.

21. The penetration testing of the TOE has been done entirely at UL's premises in Basingstoke, UK using final samples. For the repetition of the Developer's tests the Developer has sent video recordings of the automated execution of a sample selected by the Evaluator, with the corresponding logs.

22. No site visit has been performed during this evaluation. The site visit results from previous evaluations under the French Scheme have been reused, as reported in [ALC_SVR].

23. The CESG Certification Body monitored the evaluation, which was performed by the UL Transaction Security Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]/[ST-Lite]. The results of this work, completed in June 2015, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

24. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [ST]/[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.

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

Conclusions

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

Recommendations

27. 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.

Disclaimers

28. 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 on which this Certification Report is based relates only to the specific items tested.

29. 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. This report reflects the CESG Certification Body's view on that date (see paragraph 60).

30. 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.

31. 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.

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

33. 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

34. The following sections provide guidance that is of particular relevance to consumers of the TOE.

Delivery and Installation

35. 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 TOE documents detailed below:

- Section 3 of [AGD_PRE] describes the procedures for identification of the TOE.

36. No other specific security procedures are defined.

Guidance Documents

37. The guidance documentation for Personalization Phase is as follows:

- ePass ICAO essential Perso Guide, [AGD_PRE].

38. The guidance documentation for Operational Phase is as follows:

- PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, [ICAO_PKI]
- ICAO – Doc 9303 Machine Readable Travel Documents – Part 1, [ICAO_P1V1];
- ICAO – Doc 9303 Machine Readable Travel Documents – Part 3, [ICAO_P3V2];
- Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1, [BSI-TR-1];
- Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3, [BSI-TR-3].

III. EVALUATED CONFIGURATION

TOE Identification

39. The TOE is Oberthur Technologies ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0, which consists of a Machine Readable Travel Document (MRTD); a multi-applicative native software running on Infineon SLE77CLFX2400P and SLE77CLFX2407P Microcontroller and embedding ICAO application.

TOE Documentation

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

TOE Scope

41. The TOE Scope is defined in the Security Target [ST]/[ST-Lite] Section 2. The products ePass ICAO essential on SLE77 are multi-applicative native software embeddable in contact and/or contactless smart card integrated circuits of different form factors. The products can be configured to serve different use cases, during the Pre-personalization and personalization phases of the product. The product supports the storage and retrieval of structured information compliant to the Logical Data Structure as specified in [ICAO_P3V2].

TOE Configuration

42. Three different configurations of the product are defined in the [ST]/[ST-Lite] section 1.1, each of them supporting different functionality as follows:

- Config A: BAC + EAC with ECC.
- Config B: BAC + AA.
- Config C: BAC + EAC with RSA.

43. The EAC RSA functionality, as defined in the Security Target [ST]/[ST-Lite], is used in TOE configuration C.

Environmental Requirements

44. The environmental objectives for the TOE are stated in [ST]/[ST-Lite] Section 7.2.

Test Configurations

45. The Developers used this configuration for their testing:

- Config A.
- Config B.
- Config C.

46. The Evaluators used this configuration for their testing:

- Config A.
- Config B.
- Config C.

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 smart card electronic travel document according to the Logical Data Structure (LDS) defined in [ICAO9303_Part3Vol2] and supports the following security features:

- Basic Access Control protocol.
- Chip Authentication based on DH.
- Terminal Authentication based on RSA.
- Secure messaging based on TDES.
- Secure pre-personalisation and personalisation.

49. The TOE is composed of:

- the circuitry of the Infineon SLE77CLFX2400P / SLE77CLFX2407P security IC;
- the multi-applicative native software embedding ICAO application;
- the associated guidance documentation.

50. The TOE also supports other security features including EAC (with ECC) and AA, according to the configurations defined in paragraph 42.

Product Description and Architecture

51. The product is an MRTD as described in [ST]/[ST-Lite] Section 2, holding biographical data, printed data and printed portrait. It is a composite product made of a multi-applicative native software embedding ICAO application, in composition with the already certified SLE77CLFX2400P and SLE77CLFX2407P security IC from Infineon [IC_CR].

52. The logical MRTD comprises data of the MRTD holder stored according to the Logical Data Structure as detailed in [ST]/[ST-Lite] Section 2.3.

TOE Design Subsystems

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

- Application's Specific APDU Management subsystem: services to manipulate application's specific APDU commands.
- Call Back functions subsystem: specific functions needed by other subsystems and called Call Backs (CB).
- Command Dispatcher subsystem: dispatches the received commands according to the selected application.

- Application Toolbox subsystem: ensures specific application management.
- Bios Subsystem: BIOS is used to access various resources of a component, without the burden of knowing exactly how it is implemented.
- Cryptography Subsystem: provides secure cryptographic functionalities to upper-layer applications.
- IC Libraries subsystem: provided by the IC manufacturer, handles RAM variables and ROM constants.
- ID Access Conditions Management API subsystem: handles the Access Control.
- ID Authentication and Key Management API subsystem: manages the GP authentication and secure messaging, and the key diversification.
- ID BER-TLV Management API subsystem: manages the coding/decoding of TLV structures.
- ID Chip Authentication API subsystem: provides Chip Authentication.
- ID Crypto Key Management API subsystem: manages asymmetric keys storage and computation (i.e. generation, signature, verification, Diffie Hellman).
- ID File System API subsystem: manages files (i.e. elementary files, files supporting records, data objects and internal data objects).
- ID Secure Messaging API subsystem: supplies several ISO Secure Messaging APIs to protect the command-response pair, by ensuring data confidentiality and data authentication.
- ID TA Management API subsystem: provides Terminal Authentication.
- ID Cryptography toolbox API subsystem: services to manipulate cryptographic functions.
- ID Toolbox for OID handling subsystem: handles OID.
- ID Toolbox for password management subsystem: manages password such as MSK, Symmetric keys or MRZ.
- ID Secure data handling API subsystem: services to manipulate data in a secure way.
- ID Watermarking API subsystem: supplies capability to alter the portrait picture by targeted modification of the image data.
- Resident Application's Data Management subsystem: services to manipulate proprietary data.

TOE Dependencies

54. The TOE has no dependencies.

TOE Security Functionality Interfaces

55. The external TOE Security Functionality Interface (TSFI) is:

- CHANGE MSK
- CREATE FILE
- EXTERNAL AUTHENTICATE
- GET CHALLENGE
- GET DATA
- GP EXTERNAL AUTHENTICATE
- GP INITIALIZE UPDATE
- INTERNAL AUTHENTICATE
- MANAGE SECURITY ENVIRONMENT
- MUTUAL AUTHENTICATE
- PERFORM SECURITY OPERATION
- PUT DATA
- PUT KEY
- READ BINARY
- SELECT FILE
- UPDATE BINARY
- WRITE/READ LOCK

V. TOE TESTING

Developer Testing

56. 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 TOE Security Functionality;
- the TSFI, as identified in Chapter IV (in 'TOE Security Functionality Interfaces') of this report.

57. The Evaluators witnessed a sample of the Developer's security tests using video recordings of the execution of the tests and the corresponding log evidence. All the tests from the sample selected obtained a pass verdict.

Evaluator Testing

58. The Evaluators devised and ran a total of 5 independent security functional tests, different from those performed by the Developer, using the CLEF proprietary tools. No anomalies were found. The Evaluators completed these tests on 22 May 2015.

59. The Evaluators also devised and ran a total of 8 penetration tests, using the CLEF proprietary tools, to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

60. The Evaluators completed their penetration tests on 11th May 2015.

61. The samples used for both independent tests and penetration tests covered all three configurations of the TOE (Config A, B and C).

Vulnerability Analysis

62. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [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.

63. During the vulnerability analysis, a number of potential vulnerabilities were hypothesised and tested later during the penetration test phase.

64. All potential vulnerabilities identified during the analysis have been found to be not exploitable.

Platform Issues

65. The TOE is a smart card and it does not run in any Platform which is part of the environment.

VI. REFERENCES

[AGD_PRE] ePass ICAO essential Perso Guide,
Oberthur Technologies,
Issue 1, February 2015.

[AIS31] Application Notes and Interpretation of the Scheme (AIS) – 31,
Bundesamt für Sicherheit in der Informationstechnik (BSI),
AIS 31, Version 3, May 2013.

[AIS34] Application Notes and Interpretation of the Scheme (AIS) – 34,
Bundesamt für Sicherheit in der Informationstechnik (BSI),
AIS 34, Version 3, September 2009.

[ALC_SVR] OBERTHUR Development Environment Information for re-use of Sites visit (2014 campaign),
Serma Technologies,
Version 1.0, 13 March 2015.

[BSI-TR-1] Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1,
Bundesamt für Sicherheit in der Informationstechnik,
Version 2.10, 20 March 2012.

[BSI-TR-3] Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications,
Bundesamt für Sicherheit in der Informationstechnik,
Version 2.11, 12 July 2013.

[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.

[ETR] ePass ICAO essential on SLE77 - EAC RSA Evaluation Technical Report,
UL Transaction Security CLEF,
LFU/T012/ETR: UL/CC/SEC/10581005, Issue 1.0, August 2015.

[IC_CR] Certification Report BSI-DSZ-CC-0917-2014 for Infineon Technologies Security Controller M7794A12 and G12 with optional RSA2048/4096v1.02.013 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 from Infineon Technologies AG,
Bundesamt für Sicherheit in der Informationstechnik,
BSI-DSZ-CC-0917-2014, V1.0, 3 February 2014.

[ICAO_P1V1] Machine Readable Travel Documents,
Part 1, Machine Readable Passports,
Volume 1, Passports with Machine Readable Data Stored in Optical Character Recognition Format,
ICAO, Doc 9303, Sixth Edition, 2006.

[ICAO_P3V2] Machine Readable Travel Documents,
Part 3, Machine Readable Official Travel Documents,
Volume 2, Specifications for Electronically Enabled Official Travel Documents with Biometric Identification Capability,
ICAO, Doc 9303, Third Edition, 2008.

[ICAO_PKI] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access,
International Civil Aviation Organization,
Version 1.1, October 01 2004.

[JIL] Joint Interpretation Library,
(comprising [JIL_AM], [JIL_AP], [JIL_ARC] and [JIL_COMP]).

[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.

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

[PP] Machine Readable Travel Document with "ICAO Application", Extended Access Control,
BSI,
BSI-CC-PP-0056, Issue 1.10, March 2009.

[ST] Ariane - ST - EAC RSA,
Oberthur Technologies,
FQR: 110 7404, Issue 1, April 2015.

[ST-Lite] ePass ICAO essential ST lite – EAC RSA,
Oberthur Technologies,
FQR: 110 7563, Issue 1, June 2015.

[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.

[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 3.1, August 2013.

VII. ABBREVIATIONS

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

AA	Active Authentication
APDU	Application Protocol Data Unit
BAC	Basic Access Control
DH	Diffie-Hellman
EAC	Extended Access Control
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ICAO	International Civil Aviation Organization
JIL	Joint Interpretation Library
MRTD	Machine-Readable Travel Document
RSA	Rivest-Shamir-Adleman

VIII. CERTIFICATE

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

CESG Certified Product

Common Criteria

P289

This is to certify that

Oberthur Technologies

ePass ICAO essential – configuration BAC and EAC RSA, Version 1.0

running on SLE77CLFX2400P / SLE77CLFX2407P

has been evaluated under the terms of the

Common Criteria Scheme

and complies with the requirements for

Machine Readable Travel Document with "ICAO Application", Extended Access Control, v1.10

EAL4 augmented by ALC_DVS.2 and AVA_VAN.5
COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

Common Criteria

UKAS PRODUCT CERTIFICATION
0122

SOGIS IT SECURITY CERTIFIED

AUTHORISED BY	THIS PRODUCT WAS EVALUATED BY	DATE AWARDED
DIRECTOR GENERAL FOR CYBER SECURITY	UL	07/09/2015

UKAS PRODUCT CERTIFICATION
0122

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to *ISO/IEC17065:2012* 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.

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

The IT Product identified in this certificate has been evaluated at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification/Validation Report for conformance to the Common Criteria for IT Security Evaluation, version 3.1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the Common Criteria 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.
All judgements contained in this certificate, and in the associated Certification Report, are covered by the Arrangement up to EAL4, i.e. the augmentations ALC_DVS.2 and AVA_VAN.5 are not covered by the 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 Participate 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 judgements contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issues 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 judgements or for loss sustained as a result of reliance upon those judgements by a third party.
All judgements contained in this certificate, and in the associated Certification Report, are covered by the agreement.

In conformance with the requirements of ***ISO/IEC17065:2012***, 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).