0122

Common Criteria Certification Report

No. CRP301

Sealys eTravel SCOSTA-CL V4

Version MPH176

running on NXP P60D081 security controller

Issue 1.0

June 2017

NCSC Certification Body
Industry Enabling Services, NCSC,
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) requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.

Sponsor	Gemalto SA	Developer	Gemalto SA
Product Name, Version	Sealys eTravel SCOSTA-CL V4, Version MPH176		
Platform/Integrated Circuit	NXP P60D081 security controller		
Description	The product is an electronic passport application embedded in a NXP P60D081 contactless IC.		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(s) or cPP(s) Conformance	Machine Readable Travel Document with ICAO Application Basic Access Control, Version 1.10		
EAL	CC EAL 4 augmented by ALC_DVS.2		
CLEF	UL Transaction Security		
CC Certificate	P301	Date Certified	30 June 2017

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 NCSC[1] Certification Body, which is managed by the NCSC 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-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 Profile [PP] and supporting documents, CC Part 1 [CC1] and Part 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 (CCRA)

The NCSC 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[2] 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[2] 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.

[1] The UK's National Cyber Security Centre (NCSC) has absorbed and replaced CESG as the UK's national technical authority for information assurance.

[2] All judgements contained in this Certification Report are covered by the CCRA [CCRA] recognition for components up to EAL 2 only, i.e. all other components, including the augmentation ALC_DVS.2, are not covered by the CCRA. All judgements in this Certification 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 the above product at the stated version, to the Sponsor 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. Prospective consumers of the above product at the stated version 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

3. The following product completed evaluation to the CC EAL4 assurance level augmented by ALC_DVS.2 on 23 June 2017:

   Sealys eTravel SCOSTA-CL V4 Version MPH176 running on NXP P60D081 security controller.

4. The Developer was Gemalto SA.

5. The Target of Evaluation (TOE) is the Machine Readable Travel Document (MRTD) contactless IC programmed according to the Logical Data Structure (LDS) defined in [ICAO-9393] and providing the Basic Access Control (BAC) according to the ICAO document [PKI].

6. 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 'Evaluation Configuration' of this report.

7. An overview of the TOE and its product architecture can be found in Chapter IV 'TOE Architecture' of this report. Configuration requirements are specified in Section 4 of the Security Target [ST]/[ST-Lite].

Protection Profile Conformance

8. The Security Target [ST]/[ST-Lite] is certified as achieving conformance to the following protection profile:

   - Machine Readable Travel Document with ICAO Application Basic Access Control, Version 1.10 [PP].

Security Target

9. 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 those Objectives counter or meet, and the Security Functional

Requirements (SFRs) that refine the Objectives. All of the SFRs are taken from the Protection Profile [PP], which in turn are taken from CC Part 2 [CC2]; use of that standard facilitates comparison with other evaluated products.

10. The assurance requirements are taken from CC Part 3 [CC3].

11. The OSPs that must be met are specified in Section 6.4 of the Security Target [ST]/[ST-Lite].

12. The environmental objectives and assumptions regarding the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

13. The cryptographic algorithms are specified in Section 9 of the Security Target [ST]/[ST-Lite].

Evaluation Conduct

14. The NCSC 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 that work, completed in June 2017, were reported in the Evaluation Technical Report [ETR].

15. As appropriate, the evaluation used CCRA supporting documents, SOGIS supporting documents defined in [JIL], international interpretations and UK Scheme interpretations.

16. The application source code was reviewed at UL Transaction Security premises in Basingstoke (UK).

17. The Evaluator's independent security functional tests were performed at UL Transaction Security premises in Basingstoke (UK).

18. The repeat of a sample of the Developer's tests at Gemalto's Singapore premises was overseen by the Evaluator at Gemalto's Meudon (France) premises, by live videoconference, via Gemalto's internal secure communications link.

19. Penetration testing of the TOE was performed entirely at UL Transaction Security premises in Basingstoke (UK), using final samples of the TOE.

20. The site visit results from previous evaluations were reused, as detailed in the Evaluation Technical Report [ETR].

Evaluated Configuration

21. 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.

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

Conclusions

23. The conclusions of the NCSC Certification Body are summarised on page 2 ‘Certification Statement’ of this report.

Recommendations

24. Chapter II ‘TOE Security Guidance’ of this report includes recommendations on secure delivery, receipt, installation, configuration and operation of the TOE.

25. The TOE relies on the IC and its security [IC-CR]. System integrators and risk owners using the TOE should therefore make suitable arrangements to satisfy themselves that they have appropriate confidence in the mechanisms of the IC, particularly any patches and updates.

26. Any further recommendations are included in Chapter II ‘TOE Security Guidance’ of this report.

Disclaimers

27. This Certification Report and associated Certificate apply only to the specific version of the product in its evaluated configuration (i.e. the TOE). This is specified in Chapter III ‘Evaluation Configuration’ of this report. The Evaluation Technical Report [ETR], on which this Certification Report is based, relates only to the specific items tested.

28. 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 NCSC Certification Body’s view on that date (see paragraph 64 of this report).

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 TOE does not support any patching system after the TOE has been delivered to the final user.

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

32. The opinions and interpretations stated in this report under ‘Recommendations’ and ‘TOE Security Guidance’ are based on the experience of the NCSC Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

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

Delivery and Installation

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

- Section 2.3.1.1 of [UG_PRE].

Guidance Documents

35. Specific configuration advice is included in the TOE guidance documents listed in this section.

36. The User Guide and Administration Guide documentation is included in the TOE guidance documents listed in this section.

37. The guidance documentation for the Personalization phase is as follows:

- [UG_PRE] Preparation Procedures;
- [UG_PERSO] Personalization Manual.

38. The guidance documentation for the Operational phase is as follows:

- [UG_OPE] Operational User Guide.

Recommendations

39. To maintain secure operation, the consumer should follow the guidance in the documentation listed above.

III. EVALUATED CONFIGURATION

TOE Identification

40. The TOE is Sealys eTravel SCOSTA-CL V4 Version MPH176. It is a Machine Readable Travel Document (MRTD), comprising the Scosta application running on the NXP P60D081 security controller [IC-CR].

TOE Documentation

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

TOE Scope

42. The TOE Scope is defined in Section 4 of [ST]/[ST-Lite]. Functionality that is outside the TOE Scope is defined in Section 4.2 therein.

TOE Configuration

43. The evaluated configuration(s) of the TOE are defined in Section 3.2 of [ST]/[ST-Lite] and specific configuration advice is provided in the Evaluated Configuration Guide [UG_PRE].

44. The evaluated TOE configuration is composed of:

    - NXP P60D081 security controller;
    - Sealys eTravel SCOSTA-CL V4 MPH176.

Environmental Requirements

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

46. The environmental assumptions for the TOE are stated in Section 6.5 of [ST]/[ST-Lite].

Test Configurations

47. The Developer’s testing used the TOE configuration defined in Section 3.2 of [ST]/[ST-Lite].

48. The Evaluators’ testing also used the TOE configuration defined in Section 3.2 of [ST]/[ST-Lite].

IV. TOE ARCHITECTURE

Introduction

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

TOE Description and Architecture

50. The product Sealys eTravel SCOSTA-CL V4 MPH176 is an electronic passport application embedded in a NXP P60D081 contactless IC [IC-CR]. It enforces the requirements of the International Civil Aviation Organization (ICAO) and implements the Logical Data Structure (LDS) and Basic Access Control (BAC) as specified in the [ICAO-9393] document.

51. The product also conforms to the [SCOSTA-CL] specifications, as required by the Government of India. It is a native product which embeds one single application (Sealys eTravel SCOSTA-CL V4). The underlying platform is totally closed.

52. The TOE is described in Section 3.3 of [ST]/[ST-Lite].

53. The TOE is composed of the following security components:

- the application, comprising:
    - the Sealys eTravel SCOSTA-CL V4 application implemented according to the ICAO standard, with LDS and BAC as specified in the [ICAO-9393] document, and to the [SCOSTA-CL] specifications;
    - the operating system provides OS initialization, memory access, security protection, communication services and cryptographic services to the application;
- the certified platform, comprising the NXP P60D081 Integrated Circuit.

54. The following Figure 1 illustrates the TOE boundaries within the high level logical representation of the product:

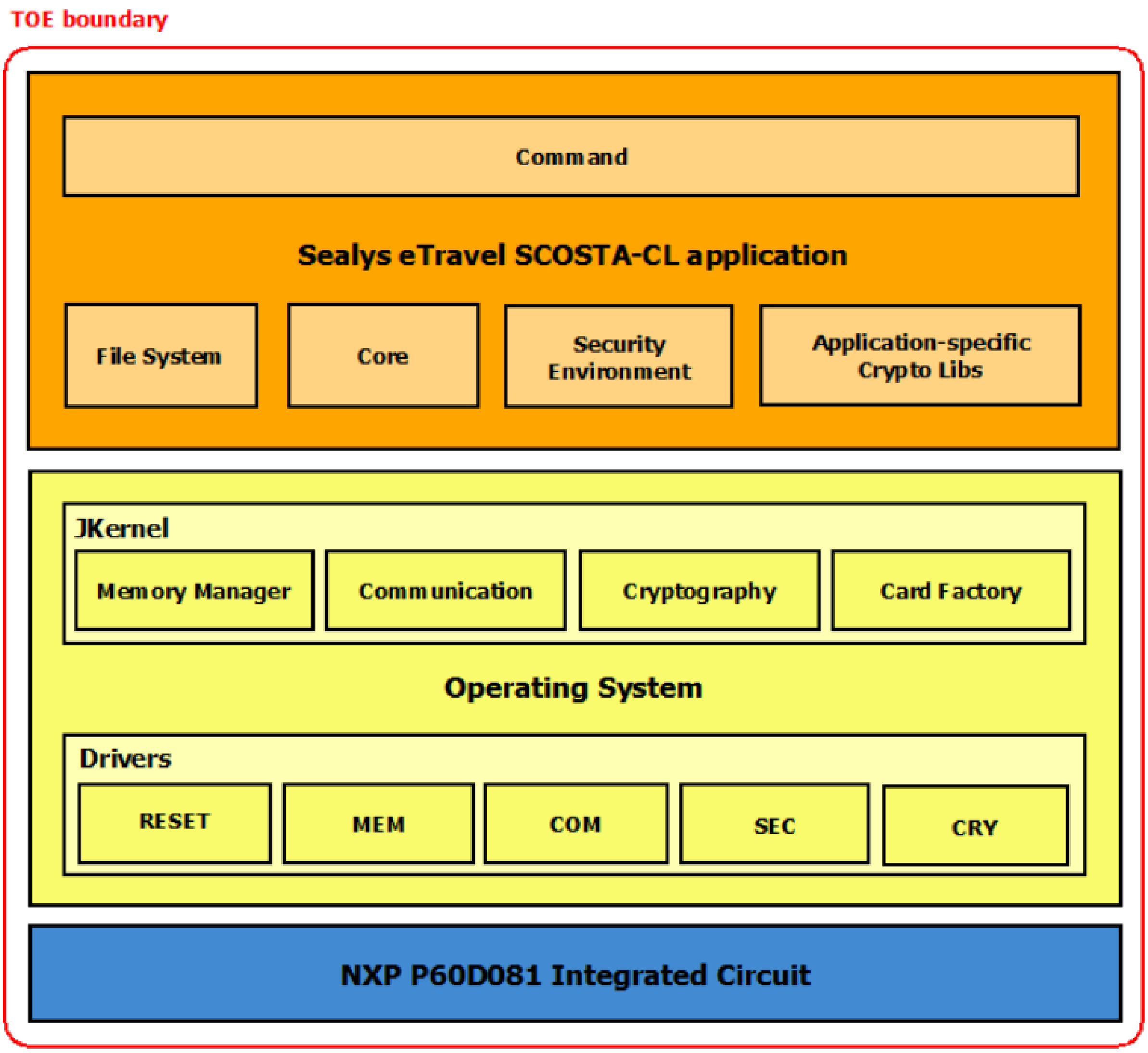

Figure 1 TOE Logical Boundaries

TOE Design Subsystems

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

- The **Driver subsystem** is in charge of secure chip initialization after reset. It also manages the memory peripherals, data exchange peripherals, cryptographic peripherals and security protection.
- The **JKernel subsystem** is in charge of OS bootstrap and OS initialization after cold/warm reset, as well as secure OS configuration. Industrialization commands such as authentication with chip makers are processed during manufacturing stage. Memory accesses, communication services and cryptography services are also managed in the JKernel subsystem, serving as an intermediate layer between the Scosta subsystem and the Driver subsystem, and providing the Application Programming Interface (API) to both of those subsystems.

- The **Scosta subsystem** provides the following services:
  - implements secure messaging mechanism such as session key derivations and algorithms for authentication, confidentiality and integrity;
  - manages binary files, record files, key files, Security Environment (SE) file, and access conditions;
  - manages the security environment of the file system;
  - implements Tag Length Value (TLV) management;
  - manages all the security architecture of the Operating System;
  - implements specific cryptographic scheme based on Scosta specification;
  - Application Protocol Data Unit (APDU) Dispatcher: processes all the Scosta commands (APDUs).

TOE Dependencies

56. The TOE has no dependencies.

TOE Security Functionality Interface

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

- APDU commands;
- electrical interface.

V. TOE TESTING

Developer Testing

58. 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.

59. 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/repeated a sample of the Developer's security tests.

60. The Developer security tests were run on the configuration defined in Chapter III 'Test Configurations'.

Evaluator Testing

61. The Evaluators devised and ran a total of 14 independent security functional tests, different from those performed by the Developer. No anomalies were found.

62. The Evaluators also devised and ran a total of 4 penetration tests to address potential vulnerabilities identified during the Vulnerability Analysis phase of the evaluation. No exploitable vulnerabilities or errors were detected.

63. The Evaluators ran their tests on the configuration defined in Chapter III 'Test Configurations'.

64. The Evaluators completed their penetration tests on 20 April 2017.

Vulnerability Analysis

65. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables. The analysis of the evaluation deliverables followed the SOGIS guidance provided in the [JIL] documentation.

Platform Issues

66. The platform relevant to the TOE is detailed in Chapter III and Chapter IV, and no platform issues were identified.

VI. REFERENCES

[CC]	Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2] and [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]	Evaluation Technical Report, UL CLEF, LFU/T023/ETR, Issue 1.0, June 2017.
[IC-CR]	NXP Secure Smart Card Controller P6021y VB including IC Dedicated Software, BSI-DSZ-CC-0955-V2-2016, Issue 1.0, October 2016.
[ICAO-9393]	9303 Part 10 and Part 11 – ICAO Machine Readable Travel Document, International Civil Aviation Organization, Seventh edition, 2015
[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 1.4, August 2015.

[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.
[PKI]	MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read Only Access, International Civil Aviation Organization, Version 1.1, 1 October 2004.
[PP]	Machine Readable Travel Document with ICAO Application Basic Access Control, BSI-CC-PP-0055, Issue 1.10, March 2009.
[SCOSTA-CL]	Specifications for the Smart-Card Operating System with Contact-less Interface, Government of India, Issue 1.0, 6 July 2007.
[ST]	Sealys eTravel SCOSTA-CL on NXP P60D081 – Security Target, Gemalto SA, Issue 1.2, 17 March 2017.
[ST-Lite]	Sealys eTravel SCOSTA-CL on NXP P60D081 – Security Target Lite, Gemalto SA, Issue 1.2p, 11 April 2017.
[UG_OPE]	Sealys eTravel SCOSTA–CL on MPH176 – V4: Operational User Guide, Gemalto SA, Issue 1.0, December 2016.
[UG_PERSO]	Personalization Manual For ScostaCL ePassport, Gemalto SA, Issue 1.6, July 2016.
[UG_PRE]	Sealys eTravel SCOSTA–CL on MPH176 – V4: Preparation procedures, Gemalto SA, Issue 1.0, December 2016.
[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 4.6, August 2016.
[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.

Standard CC abbreviations are detailed in CC Part 1 [CC1], and UK Scheme abbreviations and acronyms are detailed in [UKSP00].

APDU	Application Protocol Data Unit
API	Application Programming Interface
BAC	Basic Access Control
ICAO	International Civil Aviation Organization
JIL	Joint Interpretation Library
LDS	Logical Data Structure
LFU	CLEF UL
MRTD	Machine Readable Travel Document
SE	Security Environment
TLV	Tag Length Value
UL	Underwriters Laboratories Inc.

VIII. CERTIFICATE

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

CESG Certified Product

Common Criteria

P301

This is to certify that

Gemalto

Sealys eTravel SCOSTA-CL V4
Version MPH176

Running on NXP P60D081 security controller

has been evaluated under the terms of the

Common Criteria Scheme

and complies with the requirements for

Machine Readable Travel Document with ICAO Application Basic Access Control

Version 1.10

Common Criteria

UKAS
PRODUCT
CERTIFICATION

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

AUTHORISED BY
DIRECTOR GENERAL
FOR GOVERNMENT
AND INDUSTRY CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
UL Transaction Security

DATE AWARDED
30 June 2017

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.

The NCSC 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).

Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA)

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 NCSC or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by NCSC 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 CCRA recognition for components up to EAL2 only, i.e., all other components, including the augmentation ALC_DVS.2, 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 NCSC 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 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 Common Criteria website (http://www.commoncriteriaportal.org) 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 not be trademarks of their respective owners.

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.