122

CERTIFICATION REPORT No. CRP290

Gemalto Sealys eTravel SCOSTA–CL on G265 - V3c

running on Infineon M7820 A11 SLE78CLX802P

Issue 1.0

November 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) 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(s), Version(s)	Sealys eTravel SCOSTA–CL on G265 - V3c		
Integrated Circuit	Infineon M7820 A11 SLE78CLX802P (Certificate BSI-DSZ-CC-0829-2012, Maintenance Addendum BSI-DSZ-CC-0829-2012-MA-01)		
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” Basic Access Control [PP]		
EAL or [c]PP	EAL4 augmented by ALC_DVS.2		
CLEF	UL Transaction Security		
CC Certificate	P290	Date Certified	19th November 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 Profile [PP] and supporting documents [JIL], CC [CC] Parts 1, 2 and 3, 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 in this Certification Report are covered by the CCRA [CCRA] up to EAL2; the augmentation ALC_DVS.2 is 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 Gemalto Sealys eTravel SCOSTA–CL on G265 - V3c to the Sponsor, Gemalto SA, 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 and the Senior Officials Group - Information Systems Security (SOGIS) Mutual Recognition Agreement (MRA) [MRA] both require the Security Target (ST) to be included with the Certification Report. However Appendix I.13 and [MRA] Appendix I.13 both allow the ST to be sanitised by the removal or paraphrasing of proprietary technical information; the resulting document is named "ST-Lite". For Gemalto Sealys eTravel SCOSTA–CL on G265 - V3c, the ST is [ST] and the ST-Lite is [ST-LITE].

3. Prospective consumers of Gemalto Sealys eTravel SCOSTA–CL on G265 - V3c 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 in November 2015:

- **Gemalto Sealys eTravel SCOSTA–CL on G265 - V3c, running on Infineon M7820 A11 SLE78CLX802P**

5. The Developer was Gemalto SA.

6. The TOE is a Machine Readable Travel Document (MRTD): it is an application, including International Civil Aviation Organization (ICAO) functionality, on the Infineon M7820 A11 SLE78CLX802P Integrated Circuit (IC) Microcontroller.

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

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 (PP):

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

Security Target

11. 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 meet, and the Security Functional Requirements (SFRs) that refine the Objectives.

12. All of the SFRs are taken from [PP], which in turn are taken from CC Part 2 [CC2]; use of that standard facilitates comparison with other evaluated products.

13. All threats to the TOE are countered.

14. The OSPs that must be met are specified in [ST]/[ST-LITE] Section 4.

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

16. The cryptographic algorithms are specified in the requisites of [ST]/[ST-LITE] Section 6.

Evaluation Conduct

17. The methodology described in [CEM] was used to perform the evaluation. The TOE is a smart card product type, so the following supporting documentation from the Joint Interpretation Library (JIL) [JIL] was also used:

- 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].

18. The Evaluators reviewed the application source code and cryptographic library at the Developer's site in Meudon, France.

19. The Evaluators selected a sample of the Developer's tests. The Developer repeated its testing on that sample at its site in Singapore, witnessed by the Evaluators via videoconference, and the Developer then sent the corresponding logs to the Evaluators for verification.

20. Penetration testing of the TOE was performed entirely at UL Transaction Security's premises in Basingstoke, using final samples of the TOE.

21. No site visit was performed during this evaluation. The site visit results from previous evaluations were reused, as detailed in the Evaluation Technical Report [ETR].

22. 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 the evaluation, completed in November 2015, were reported in the ETR [ETR].

Evaluated Configuration

23. 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.

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

Conclusions

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

Recommendations

26. 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

27. 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.

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 CESG Certification Body's view on that date (see paragraph 56).

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

30. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. However, note that unevaluated

patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

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

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

II. TOE SECURITY GUIDANCE

Introduction

33. The following sections provide guidance of particular relevance to 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 below:

- Preparation Procedures [AGD_PRE] Section 2.3.1 describes the procedures for identification of the TOE.

35. No other specific security procedures are defined.

Guidance Documents

36. The guidance documentation provided for administrators during the manufacturing, personalisation and usage phases is as follows:

- Preparation Procedures [AGD_PRE];
- Personalisation Manual [AGD_P_MAN];
- Operational User Guide [AGD_OPE].

III. EVALUATED CONFIGURATION

TOE Identification

37. The TOE is Gemalto Sealys eTravel SCOSTA–CL on G265 - V3c. It is a MRTD, comprising the Scosta application running on the Infineon M7820 A11 SLE78CLX802P IC Microcontroller.

TOE Documentation

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

TOE Scope

39. The TOE Scope is defined in the Security Target [ST]/[ST-LITE], Section 1. The TOE includes the hardware platform, the Infineon Microcontroller on which the operating system is implemented, and some dedicated IC support software. The Scosta application is the only application within the TOE scope. The TOE boundary is illustrated in Figure 1 below.

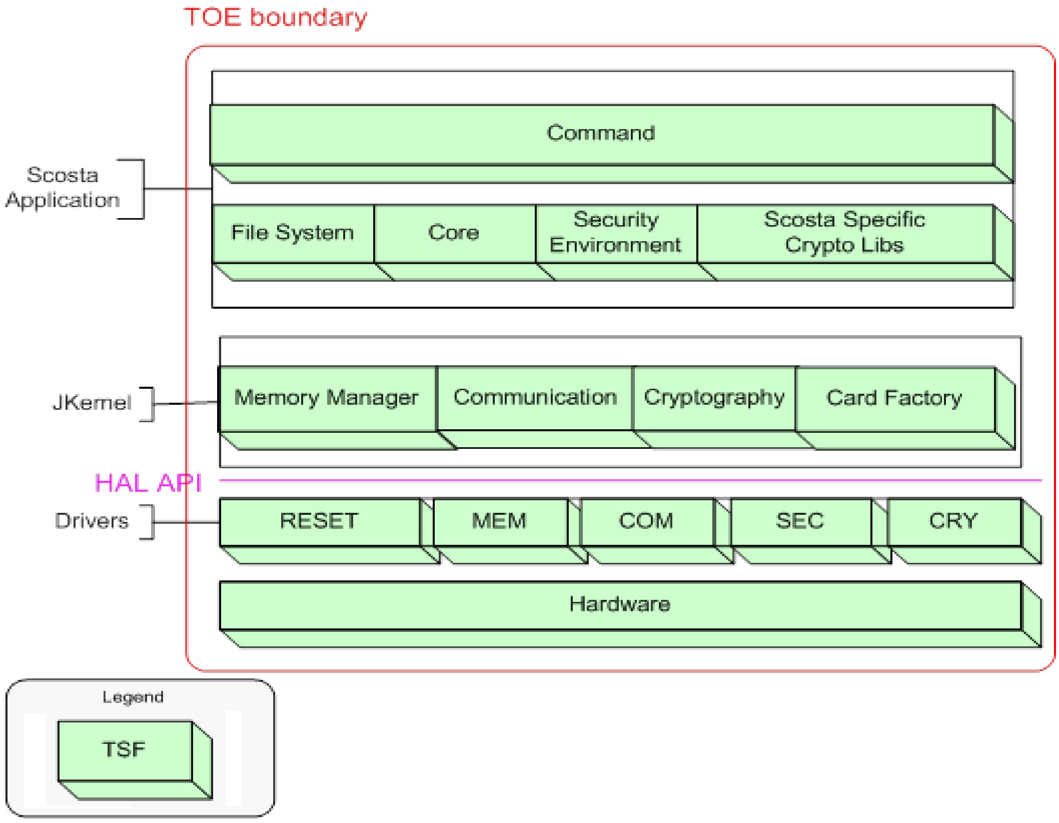

Figure 1 - TOE Boundary

TOE Configuration

40. The TOE configuration is described in the Security Target [ST]/[ST-LITE] Sections 1.5 and 1.6. The TOE is the whole product, as opposed to a specific configuration of a product.

Environmental Requirements

41. The environmental objectives for the TOE are stated in [ST]/[ST-LITE] Section 4.2.

Test Configurations

42. There are no different TOE configurations other than the one defined in the Security Target [ST]/[ST-LITE]. The Evaluators therefore used the same test configurations as the Developer.

43. The only test configuration is related to the personalised profiles that can be used in the operational phase with BAC functionalities.

IV. PRODUCT ARCHITECTURE

Introduction

44. 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.

45. The TOE is a smart card electronic travel document according to the Logical Data Structure (LDS) defined in [ICAO9303] and supports the following security features:

- Basic Access Control protocol;
- Secure messaging based on MacAlgo3 and TDES;
- Secure pre-personalisation and personalisation.

Product Description and Architecture

46. The product is a MRTD as described in [ST]/[ST-LITE] Section 1.5, holding biographical data, printed data and printed portrait. It is a composite product, comprising the Scosta application and the already-certified Infineon M7820 A11 SLE78CLX802P security IC [CR].

47. The logical MRTD comprises data of the MRTD holder stored according to the LDS as detailed in [ST]/[ST-LITE] Section 1.5.2.

48. The TOE is delivered in the manufacturing phase to the MRTD manufacturer as a microcontroller module, including the IC Embedded Software in the non-volatile programmable memories and the TOE application, together with the guidance documentation.

TOE Design Subsystems

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

- Scosta subsystem: manages general services (Application Protocol Data Unit (APDU) dispatcher, secure messaging, files, security environment, security architecture and some cryptographic functionality).
- JKernel subsystem: serves as an intermediate layer between the Scosta subsystem and the Driver subsystem; in charge of the OS configuration and memory access.
- Driver subsystem: in charge of secure chip initialization after reset; manages the memory peripherals, data exchange peripherals, cryptographic peripherals and security protection.

TOE Dependencies

50. The TOE has no dependencies.

TOE Security Functionality Interfaces

51. The external TOE Security Functionality Interface (TSFI) is provided by the following APDU commands:

- SELECT FILE;
- READ BINARY;
- UPDATE BINARY;
- ERASE BINARY;
- WRITE BINARY;
- READ RECORD;
- UPDATE RECORD;
- APPEND RECORD;
- WRITE RECORD;
- CREATE FILE;
- DELETE FILE;
- ACTIVATE FILE;
- DEACTIVATE FILE;
- TERMINATE DF;
- TERMINATE EF;
- TERMINATE CARD USAGE;
- VERIFY;
- CHANGE REFERENCE DATA;
- RESET RETRY COUNTER;
- ENABLE VERIFICATION REQUIREMENT;
- DISABLE VERIFICATION REQUIREMENT;
- PSO DECIPHER;
- PSO ENCIPHER;
- PSO COMPUTE CC;
- PSO VERIFY CC;
- PSO HASH;
- GET CHALLENGE;
- INTERNAL AUTHENTICATE;
- EXTERNAL AUTHENTICATE;
- MUTUAL AUTHENTICATE;
- MSE SET;
- MSE RESTORE;
- GET DATA;
- PUT DATA;
- GET RESPONSE;
- MSE STORE;
- MSE ERASE.

V. TOE TESTING

Developer Testing

52. 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.

53. 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 sample of the Developer's security tests via videoconference, checked the corresponding log evidence and verified that all tests had successfully passed.

Evaluator Testing

54. The Evaluators devised and ran a total of 12 independent security functional tests, different from those performed by the Developer, using the Developer's tools. No anomalies were found. The Evaluators completed those tests on 3rd September 2015.

55. The Evaluators also devised and ran a total of 3 penetration tests, using their CLEF-proprietary tools, to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

56. The Evaluators completed their penetration tests on 24th July 2015.

Vulnerability Analysis

57. 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, particularly the source code.

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

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

Platform Issues

60. The TOE is a smart card and does not run on any platform in the environment.

VI. REFERENCES

[AGD_OPE] ScostaCL V3C BAC: Operational User Guide,
Gemalto SA,
D1341110, Version 0.4, 23rd October 2015.

[AGD_PRE] ScostaCL V3C BAC: Preparation Procedures,
Gemalto SA,
D1341111, Version 0.5, 30th October 2015.

[AGD_P_MAN] Personalization Manual For ScostaCL ePassport,
Gemalto SA,
D1338461, Version 1.6, 30th October 2015.

[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.

[CR] Certification Report for Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software,
Bundesamt für Sicherheit in der Informationstechnik (BSI),
BSI-DSZ-CC-0829-V2-2015, 3rd August 2015.

[ETR] Evaluation Technical Report: LFU/T017,
UL Transaction Security CLEF,
UL/CC/SEC/10777972, Issue 1.2, 18th November 2015.

[ICAO9303] Machine Readable Travel Documents,
Part 3, Machine Readable Official Travel Documents,
Volume 2, Specifications for Electronically Enabled MRTDs with Biometric Identification Capability,
ICAO, Doc 9303, Third Edition, 2008.

[JIL] Joint Interpretation Library documents
[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 1.3, February 2015.

[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.

[PP] Machine Readable Travel Document with “ICAO Application”,
Basic Access Control,
Bundesamt für Sicherheit in der Informationstechnik (BSI),
BSI-CC-PP-0055, Issue 1.10, 25th March 2009.

[ST] Gemalto Sealys eTravel SCOSTA-CL on G265-V3c Security Target,
Gemalto SA,
D1340139, Version 1.8, 30th October 2015.
(Note: That is a proprietary, in-confidence document.)

[ST-LITE] Gemalto Sealys eTravel SCOSTA-CL on G265-V3c Security Target Lite,
Gemalto SA,
D1375202, Version 1.3, 30th October 2015.
(Note: That is a public, sanitised document.)

[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].

APDU	Application Protocol Data Unit
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationstechnik
DES	Data Encryption Standard
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
JIL	Joint Interpretation Library
LDS	Logical Data Structure
LFU	Commercial Evaluation Facility - UL
MRA	Mutual Recognition Agreement
MRTD	Machine-Readable Travel Document
SOGIS	Senior Officials Group
TDES	Triple DES
UL	Underwriters Laboratories Inc.

VIII. CERTIFICATE

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

CESG Certified Product

Common Criteria

P290

This is to certify that

Gemalto SA

Sealys eTravel SCOSTA–CL on G265 - V3c

running on Infineon M7820 A11 SLE78CLX802P

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, v1.10

EAL4 augmented by ALC_DVS.2
COMMON CRITERIA (ISO/IEC 15408) ASSURANCE LEVEL

Common Criteria

UKAS
PRODUCT
CERTIFICATION
0122

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

AUTHORISED BY
DIRECTOR GENERAL
FOR CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
UL Transaction Security

DATE AWARDED
19th November 2015

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.

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/IEC 17065:2012* 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 in this certificate, and in the associated Certification Report, are covered by the Arrangement up to EAL2; the augmentation ALC_DVS.2 is 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 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 in this certificate, and in the associated Certification Report, are covered by the Agreement.

In conformance with the requirements of *ISO/IEC 17065:2012*, 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).

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.