122

CERTIFICATION REPORT No. CRP284

IDProtect Duo (in EAC configuration)
Version 10
running on Inside Secure AT90SC28880RCFV2

Issue 1.0

July 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	Athena Smartcard, Inc	Developer	Athena Smartcard, Inc
Product(s), Version(s)	IDProtect Duo v10 (in EAC configuration)		
Integrated Circuit	Inside Secure AT90SC28880RCFV2 Certificate: BSI-PP-0002-2001		
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	EAL5 augmented by ALC_DVS.2 and AVA_VAN.5		
CLEF	UL Transaction Security		
CC Certificate	P284	Date Certified	10th July 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 Protection Profiles [PP] and supporting documents [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 [MRA] up to EAL5. 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 Athena IDProtect Duo v10 (in EAC configuration) to the Sponsor, Athena Smartcard Inc, 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 Athena IDProtect Duo v10 (in EAC configuration), the ST is [ST] and the ST-Lite is [ST-Lite].

3. Prospective consumers of Athena IDProtect Duo v10 (in EAC configuration) should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

4. The following product completed evaluation to CC EAL5 assurance level augmented by ALC_DVS.2 and AVA_VAN.5 in July 2015:

   - **Athena IDProtect Duo v10 (in EAC configuration) running on Inside Secure AT90SC28880RCFV2**

5. The Developer was Athena Smartcard, Inc.

6. The TOE is a Machine Readable Travel Document (MRTD): a Java Card on Inside Secure AT90SC28880RCFV2 Microcontroller embedding ICAO applet.

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: Machine Readable Travel Document with "ICAO Application", Extended 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 these 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 this 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 [ST]/[ST-Lite] Section 1.9.5.

Evaluation Conduct

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

18. The application source code and cryptographic library have been reviewed by UL Transaction Security's premises in Basingstoke.

19. The penetration testing of the TOE has been performed entirely at UL Transaction Security's premises in Basingstoke, using final samples of the TOE. For the repetition of the Developer's tests two approaches have been followed:

- For all the tests except for the proprietary applet tests, a sample of tests was selected to be repeated in Athena's site in Livingston, UK, and witnessed by the Evaluator.

- For the applet proprietary tests, the Evaluator selected a subset of tests and the Developer sent video recordings of the automated execution of that sample together with the corresponding logs.

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

21. 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 July 2015, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

22. 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.

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

Conclusions

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

Recommendations

25. 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

26. 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.

27. 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 55).

28. 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.

29. 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.

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

31. 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

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

Delivery and Installation

33. 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 6 of [AGD_PRE] describes the procedures for identification of the TOE.

34. No other specific security procedures are defined.

Guidance Documents

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

- Manufacturer Manual [AGD_MAN];
- Preparation Manual [AGD_PRE];
- Operation Manual [AGD_OPE].

III. EVALUATED CONFIGURATION

TOE Identification

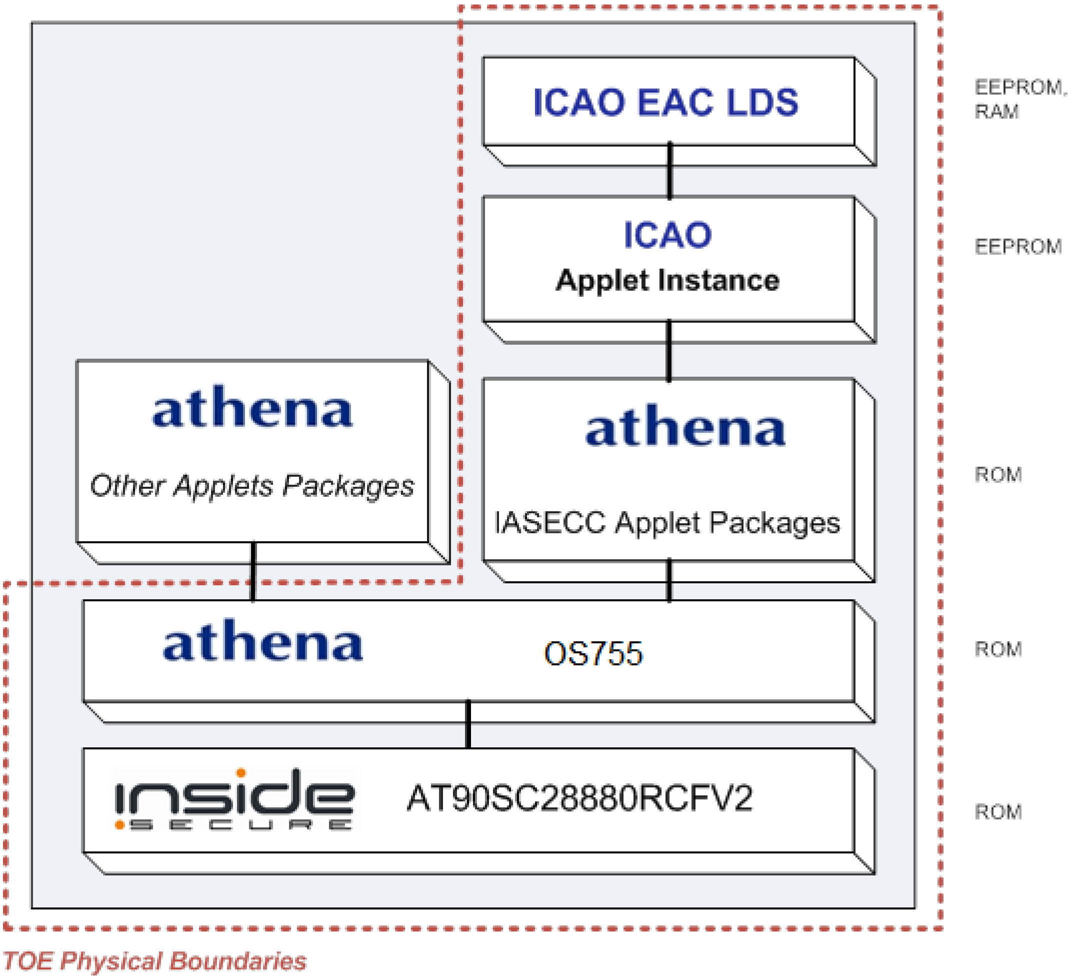
36. The TOE is Athena Protect Duo v10 (in EAC configuration), which consists of a Machine Readable Travel Document (MRTD): a Java Card on Inside Secure AT90SC28880RCFV2 Microcontroller embedding ICAO applet.

TOE Documentation

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

TOE Scope

38. The TOE Scope is defined in the Security Target [ST]/[ST-Lite] Section 1. The TOE includes the hardware platform, the Inside Secure Microcontroller, on which the operating system is implemented, and some dedicated IC support software. The only applet within the TOE scope is the ICAO BAC applet.



TOE Configuration

39. The TOE configuration is described in the Security Target [ST]/[ST-Lite] Section 1.5. The TOE is the whole product, as opposed to a specific configuration of a product.

Environmental Requirements

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

Test Configurations

41. There are no different TOE configurations other than the one defined in the Security Target [ST]/[ST-Lite].

42. The two test configurations are related to the two personalised profiles that can be used in the operational phase: one with BAC, EAC (with RSA) and Active Authentication; the other with BAC, EAC (with Elliptic Curves) and Active Authentication.

IV. PRODUCT ARCHITECTURE

Introduction

43. 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.

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

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

Product Description and Architecture

45. The product is an MRTD as described in [ST]/[ST-Lite] Section 1.5, holding biographical data, printed data, printed portrait and biometric information. It is a composite product made of the IASECC Applet running on the Athena IDProtect dual interface Java Card operating system, both in composition with the already certified AT90SC28880RCFV2 security IC from Inside Secure [CR].

46. The logical MRTD comprises data of the MRTD holder stored according to the Logical Data Structure as detailed in [ST]/[ST-Lite] Section 1.5.2.

47. 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 MRTD application, together with the guidance documentation.

TOE Design Subsystems

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

- Dispatcher Subsystem – provides general Java Runtime services; receives APDUs and handles them directly or dispatches them to the selected Applet.

- Applets Subsystem – comprises the ICAO applet functionality; contains Applets, the user application code of the system. Note that the ISD (Issuer Security Domain) behaves as an applet.

- Issuer Security Domain Subsystem – corresponds to the Issuer Security Domain as specified in Global platform.

- JavaCard (Java Card) Subsystem – provides the public services specified by Java Card and other APIs, as well as private services specified by Global Platform for the ISD and the Card Manager. It is split in two to facilitate the visualization of the Virtual Machine component as it operates in the background of the Java code.

- Card Manager Subsystem – the representative of the Card Issuer; provides the capability for loading, installing and deleting applications that belong to either the Card Issuer or other Application Providers. The Card Manager contains the library of modules that provide the Open Platform Environment. These modules, only available to the ISD, comprise the public Global Platform services for the management of Delegation, Secure Channels, Card Content and Card Lifecycle.

- OS (Operating System) Subsystem – provides OS-level services, including cryptographic and I/O services, to the rest of the system, especially for the Java Card Runtime Environment.

- Kernel Run Time Subsystem – provides general and utility services to all other subsystems in the areas of memory management, heap and transactions.

- KPL (Kernel Porting Subsystem) – provides a common interface to hardware services; contains the “platform-specific” code which controls the special cryptographic, security, IO, and memory hardware of the chip. Replacing this layer allows the rest of the system to be ported to different kinds of chip hardware.

- Chip Hardware – the CPU, memory and coprocessors which perform the operations.

TOE Dependencies

49. The TOE has no dependencies.

TOE Security Functionality Interfaces

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

- COMMIT PERSO (ACTIVATE)
- CREATE SDO
- CREATE FILE
- DELETE SDO
- DELETE FILE
- EXTERNAL AUTHENTICATE (manufacturing)
- GENERATE ASYMMETRIC KEYPAIR
- GET CHALLENGE
- GET DATA
- GET RESPONSE
- INTERNAL AUTHENTICATE

- MSE – SET AT
- MSE – SET DST
- MSE – SET KAT
- MUTUAL AUTHENTICATE
- PSO – VERIFY CERTIFICATE
- PUT DATA
- READ BINARY
- SELECT FILE
- UPDATE BINARY
- INSTALL CERTIFICATE (PUT DATA)
- INITIALIZE UPDATE
- EXTERNAL AUTHENTICATE
- INSTALL (for Registry Update).

V. TOE TESTING

Developer Testing

51. 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.

52. 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 using video and corresponding log evidence and all tests were successfully passed.

Evaluator Testing

53. 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 these tests on 16 February 2015.

54. The Evaluators also devised and ran a total of 9 penetration tests, using their CLEF-proprietary tools, to address potential vulnerabilities considered during the evaluation. They used two profiles on the smart cards, where the only difference in configuration is the type of algorithm run during Chip Authentication. No exploitable vulnerabilities or errors were detected.

55. The Evaluators completed their penetration tests on 19th December 2014.

Vulnerability Analysis

56. 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.

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

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

Platform Issues

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

VI. REFERENCES

[AGD_MAN] IDProtect Duo v10 ICAO - Manufacturer Manual,
Athena Smartcard Inc,
Version 1.0, March 2015.

[AGD_OPE] Athena IDProtect Duo v10 – ICAO EAC Operation Manual,
Athena Smartcard Inc,
Version 1.0, March 2015.

[AGD_PRE] IDProtect Duo v10 ICAO EAC - Preparation Manual,
Athena Smartcard Inc,
Version 1.0, March 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

[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] Common Criteria Surveillance Report No. ANSSI-CC-2013/59-S01,
Agence Nationale de la Sécurité des Systèmes D'information,
ANSSI-CC-SUR-F-08/004, 13th January 2015.

[ETR] IDProtect Duo v10 Evaluation Technical Report,
UL Transaction Security CLEF,
LFU/T009/ETR: UL/CC/SEC/10424551, Issue 1.3, 9th July 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,
(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, 8th 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] Athena IDProtect Duo v10 ICAO EAC optional Active Authentication Security Target,
Athena Smartcard Inc,
IDP10-STEAC-01, Version 1.4, July 2015.

[ST-Lite] Athena IDProtect Duo v10 ICAO EAC optional Active Authentication Security Target Lite,
Athena Smartcard Inc,
IDP10-STEAC-02, Version 1.4, July 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].

APDU	Application Protocol Data Unit
EAC	Extended Access Control
DH	Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
IASECC	Identification Authentication Signature – European Citizen Card
ICAO	International Civil Aviation Organization
ISD	Issuer Security Domain
JIL	Joint Interpretation Library
MRTD	Machine-Readable Travel Document

VIII. CERTIFICATE

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

CESG

CESG CERTIFICATION BODY

CERTIFICATE No.
P284

This Certificate confirms that

Athena IDProtect Duo v10 (in EAC configuration)

running on Inside Secure AT90SC28880RCFV2

has been evaluated under the terms of the

UK IT Security Evaluation and Certification Scheme

and complies with the requirements for

EAL5 augmented by ALC_DVS.2 and AVA_VAN.5

COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

and Protection Profile:

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

The scope of the evaluated functionality was as claimed by the Security Target
and as confirmed by the associated Certification Report **CRP284**.

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

ASSURED PRODUCTS CESG IACS ASSURED SYSTEMS

Common Criteria ®

SOGIS IT SECURITY CERTIFIED

UKAS PRODUCT CERTIFICATION
122

AUTHORISATION
Director for Information Assurance

DATE
10 July 2015

122

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; 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 EAL5, 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 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 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***, and CC Supporting Documents as listed in the Certification Report 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 listed in this certificate 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 ***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 be trademarks of their respective owners.