122

CERTIFICATION REPORT No. CRP278

SOMA-c004 e-Passport (BAC)

Version 1.0

running on Infineon M7892 Integrated Circuit

Issue 1.0

December 2014

CESG Certification Body
IA Service Management, 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	Arjo Systems - Arjowiggins Security - Gep		
Developer	Arjo Systems - Arjowiggins Security - Gep		
Product, Version	SOMA-c004 e-Passport (BAC), v1.0		
Integrated Circuit	Infineon M7892 (Certificate: BSI-DSZ-CC-0782-2012)		
Description	Electronic Passport		
CC Version	Version 3.1 release 4		
CC Part 2	Conformant	CC Part 3	Conformant
PP Conformance	Machine Readable Travel Document with "ICAO Application", Basic Access Control (BAC PP)		
EAL	EAL4 augmented by ALC_DVS.2		
CLEF	UL Transaction Security		
CC Certificate	P278	Date Certified	23rd December 2014

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]/[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 Parts 1 [CC1] and 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 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 report are covered by the SOGIS MRA [MRA]. All judgements contained in this report are covered by the CCRA [CCRA] up to EAL4, i.e. the augmentation *ALC_DVS.2* is not covered by the CCRA.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of SOMA-c004 e-Passport (BAC) v1.0 to the Sponsor, Arjo Systems - Arjowiggins Security - Gep, 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 SOMA-c004 e-Passport (BAC) v1.0, the ST is [ST] and the ST-lite is [ST_LITE].

3. Prospective consumers of SOMA-c004 e-Passport (BAC) v1.0 should understand the specific scope of the certification by reading this report in conjunction with the ST-lite [ST_LITE], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

4. The following product completed evaluation to CC EAL4 assurance level augmented by ALC_DVS.2 in December 2014:

- **SOMA-c004 e-Passport (BAC) v1.0 running on Infineon M7892 Integrated Circuit.**

5. The Developer was Arjo Systems - Arjowiggins Security - Gep.

6. The TOE is an Electronic Passport (ePassport) product which supports security features including Basic Access Control (BAC), covered by the ST [ST]/[ST_LITE] and this Certification Report.

Note: The TOE also supports other security features, including Extended Access Control (EAC), Supplemental Access Control (SAC) and Active Authentication (AA), which are covered by a separate ST/ST-lite and a separate Certification Report [CR_EAC].

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

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’s architecture is provided in Chapter IV ‘Product Architecture’ of this report.

Protection Profile Conformance

10. The ST [ST]/[ST_LITE] achieved conformance to the following Protection Profile (PP):

- Machine Readable Travel Document with “ICAO Application”, Basic Access Control (BAC PP) [PP_BAC].

Security Target

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

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

13. All threats to the TOE are countered.

14. The SFRs in the ST [ST]/[ST_LITE] are taken from the PP, which facilitates comparison with other evaluated products.

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

Evaluation Conduct

16. The methodology described in [CEM] has been used to conduct the evaluation. The TOE is a smartcard product type, so additional supporting documentation related to the Joint Interpretation Library (JIL) has been used as follows:

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

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

18. As agreed in advance with the CESG Certification Body, the Evaluators reused the site visit results from a previous evaluation under the French Scheme.

19. 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 ST [ST]/[ST_LITE]. The results of this work, completed in December 2014, were reported in the Evaluation Technical Report (ETR) [ETR].

Evaluated Configuration

20. The TOE should be used in accordance with the environmental assumptions specified in the ST [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.

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

Conclusions

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

Recommendations

23. 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

24. 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 'Evaluated Configuration' of this report. The ETR on which this Certification Report is based relates only to the specific items tested.

25. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed. This report reflects the CESG Certification Body's view on that date (see paragraph 57).

26. 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.

27. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

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

29. Note that the opinions and interpretations stated 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

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

Delivery and Installation

31. On receipt of the TOE, the consumer 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:

- Section 7.1 of [AGD_PRE] describes the procedures for identification of the TOE.

32. No other specific security procedures are defined.

Guidance Documents

33. The guidance documentation [AGD] is as follows:

- Pre-personalization Guidance [AGD_PRE];
- Personalization Guidance [AGD_OPE];
- User Guidance [AGD_UG].

III. EVALUATED CONFIGURATION

TOE Identification

34. The TOE is SOMA-c004 e-Passport (BAC) v1.0, which consists of the SOMA-c004 Operating System in composition with the already-certified security M7892 integrated circuit (IC) from Infineon Technologies [CR_INF].

35. The microcontroller module is ready to be integrated into the inlay with the antenna and substrate, which are outside the physical boundaries of the TOE.

TOE Documentation

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

TOE Scope

37. The TOE Scope is defined in the ST [ST]/[ST_LITE] Section 1.5. The TOE is delivered at the end of phase 2, so Pre-personalization (phase 2), Personalization (phase 3) and final usage (phase 4) occur after that delivery.

TOE Configuration

38. The TOE is the whole product, as opposed to a specific configuration of a product.

Environmental Requirements

39. The TOE environmental objectives are stated in the ST [ST]/[ST_LITE] Section 4.2.

40. The TOE does not rely on the environment to operate securely in final usage.

Test Configurations

41. There are no different configurations.

IV. PRODUCT ARCHITECTURE

Introduction

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

Product Description and Architecture

43. The TOE is an Electronic Passport smartcard product, i.e. a Machine Readable Travel Document (MRTD), in accordance with the Logical Data Structure (LDS) defined in [ICAO].

44. The TOE is a composite product, composed of the SOMA-c004 operating system (OS) and the MRTD software application providing the passport features, running in composition with the already-certified Infineon M7892 IC from Infineon Technologies [CR_INF]. The TOE is composed of:

- the circuitry of the MRTD's chip M7892;
- the IC Dedicated Software with the parts *IC Dedicated Test Software* and *IC Dedicated Support Software*;
- the IC Embedded Software (SOMA-c004 OS);
- the MRTD application;
- the associated guidance documentation [AGD].

45. The OS and the application were developed by Arjo Systems - Arjowiggins Security - Gep.

46. The TOE adds security features to a passport booklet, providing machine-assisted identity confirmation and machine-assisted verification of document security, including the following features:

- BAC, according to [ICAO];
- secure messaging;
- secure pre-personalisation and personalisation.

47. Cryptographic techniques are applied to confirm the identity of the holder and to verify the authenticity of the passport.

48. The TOE also supports other security features, including EAC, SAC and AA, which are covered by a separate ST/ST-lite and a separate Certification Report [CR_EAC].

TOE Design Subsystems

49. The high-level TOE subsystems, and their security features/functionality, are composed of the already-certified secure microcontroller [CR_INF] and the following subsystems:

- S1 – Commands Manager:

  This subsystem is responsible for card commands (ISO 7816, Card Personalisation Specification (CPS), other proprietary commands) and access control verification.

- S2 – Security Manager:

  This subsystem provides the following services:

  i. Authentication of external entities throughout initialisation, pre-personalisation, personalisation and operational life cycle phases.

  ii. The CPS mechanism.

  iii. Secure messaging.

  iv. Security data management, protection of assets (e.g. cryptographic keys) and sensitive attributes (e.g. retry counters).

  v. Security environment management.

  vi. Cryptographic primitive abstraction layer, using the cryptographic services provided by the underlying IC.

- S3 – Data Object and Non Volatile Memory (NVM) Management:

  This subsystem provides persistent object management, such as the file system and other persistent data belonging to the OS. It also implements the low level NVM management.

- S4 – Communications Manager:

  This subsystem provides contactless communication and handles interruptions, such as security failure interruption.

- S5 – Initialization and Card Management:

  This subsystem provides the initialisation of the TSF, the main dispatching loop, preparation of response data such as status words and other auxiliary utility functions (e.g. data type conversion, checksum computation, memory copy, memory comparison).

TOE Dependencies

50. The TOE has no dependencies.

TOE Security Functionality Interfaces

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

- Application Protocol Data Unit (APDU) commands supported by the TOE in phases 2, 3 and 4 are described in the TOE operational guidance identified in Chapter II (in 'Guidance Documents') of this report.

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 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, at the Developer’s premises.

54. The Developer tested the APDU directly in the final TOE. Internal functionality of the OS was tested using an emulator.

Evaluator Testing

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

56. The Evaluators also devised and ran a total of 7 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

57. The Evaluators completed their penetration tests on 4th July 2014.

Vulnerability Analysis

58. 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 of the OS.

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

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

Platform Issues

61. The TOE is a smartcard and does not run in any Platform which is part of the environment.

VI. REFERENCES

[AGD] Guidance documentation, consists of the following documents:
AGD_PRE Pre-personalization Guide [AGD_PRE];
AGD_OPE Personalization Guide [AGD_OPE];
AGD_UG User Guide [AGD_UG].

[AGD_OPE] Personalization Guidance for SOMA-c004 electronic passport,
Arjo Systems - Arjowiggins Security - Gep,
TCAE140007 , Issue 1.0, 28th January 2014.

[AGD_PRE] Pre-personalization Guidance for SOMA-c004 electronic passport,
Arjo Systems - Arjowiggins Security - Gep,
TCAE140006, Issue 1.0, 14th July 2014.

[AGD_UG] User Guidance for SOMA-c004 electronic passport,
Arjo Systems - Arjowiggins Security - Gep,
TCAE130041, Issue 1.0, 28th January 2014.

[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_EAC] Certification Report No. CRP279: SOMA-c004 e-Passport (EAC-SAC-AA),
CESG Certification Body,
UK IT Security Evaluation and Certification Scheme,
CRP279, Issue 1.0, December 2014.

[CR_INF] Common Criteria Certification Report No. BSI-DSZ-CC-0782-2012,
Bundesamt für Sicherheit in der Informationstechnik,
BSI-DSZ-CC-0782-2012, Issue 1.0, 15th June 2007.

[ETR] Evaluation Technical Report,
UL Transaction Security CLEF,
LFU/T005/ETR, Issue 1.1, December 2014.

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

[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_BAC] Common Criteria Protection Profile: Machine Readable Travel Document with “ICAO Application”, Basic Access Control,
Bundesamt für Sicherheit in der Informationstechnik,
BSI-CC-PP-0055, Version 1.10, 25th March 2009.

[ST] Security Target for SOMA-c004 Electronic Passport, Basic Access Control,
Arjo Systems - Arjowiggins Security - Gep,
TCAE130040, Issue 1.5, 17th November 2014.

[ST_LITE] Security Target for SOMA-c004 Electronic Passport, Basic Access Control, Public Version,
Arjo Systems - Arjowiggins Security - Gep,
TCLE140041, Issue 1.1, 17th November 2014.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.8, August 2013.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.5, August 2013.

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

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 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
CLEF	Commercial Evaluation Facility
CPS	Card Personalisation Specification
EAC	Extended Access Control
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
JIL	Joint Interpretation Library
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
NVM	Non Volatile Memory
SAC	Supplemental Access Control

VII. CERTIFICATE

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

CESG CERTIFICATION BODY

CERTIFICATE No.

P278

This Certificate confirms that

Arjo Systems - Arjowiggins Security - Gep SOMA c004 e-Passport (BAC) v1.0

running on Infineon M7892 Integrated Circuit

has been evaluated under the terms of the

UK IT Security Evaluation and Certification Scheme

and complies with the requirements for

EAL4 augmented by ALC_DVS.2

COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

and Protection Profile:

Machine Readable Travel Document with “ICAO Application”, Basic 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 **CRP278**.

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.

AUTHORISATION

Director for Information Assurance

DATE

23 December 2014

122

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.

Standard: 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), 2nd July 2014

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

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

Senior Officials Group – Information Systems Security (SOGIS)
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgments contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

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

The IT product identified in this certificate has been evaluated by the UL Transaction Security Commercial Evaluation Facility (an accredited and approved Evaluation Facility of the UK) using the ***Common Methodology for Information Technology Security Evaluation***, ***Version 3.1*** 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 expressed or implied.

In conformance with the requirements of ***ISO/IEC 17065:2012***, ***CCRA*** and ***SOGIS MRA***, the CESG Certification Body's website (www.cesg.gov.uk) provides additional information:

- type of IT product (i.e. product category); and
- details of IT 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.