122

CERTIFICATION REPORT No. CRP277

ECC CPU card

Version 1.2

running on SLE77CLFX2407PM

Issue 1.0

October 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	Gemalto	Developer	Gemalto
Product, Version	ECC CPU card v1.2		
Integrated Circuit	SLE77CLFX2407PM (M7794) *(CC certificate no. BSI-DSZ-CC-0883)*		
Description	Electronic Purse		
CC Version	Version 3.1 release 4		
CC Part 2	Conformant	CC Part 3	Conformant
PP Conformance	None		
EAL	EAL4 augmented by AVA_VAN.5 and ALC_DVS.2		
CLEF	UL Transaction Security		
CC Certificate	P277	Date Certified	19 October 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], 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 CC Parts 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM], Supporting Documents 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 augmentations AVA_VAN.5 and ALC_DVS.2 are 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 ECC CPU card Version 1.2 to the Sponsor, Gemalto, 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. [CCRA] Appendix I.13 allows the ST to be sanitised by removing or paraphrasing proprietary technical information; the resulting document is named "ST-lite". For ECC CPU card Version 1.2, the ST is [ST] and the ST-lite is [ST_LITE].

3. Prospective consumers of ECC CPU card Version 1.2 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 AVA_VAN.5 and ALC_DVS.2 in September 2014:

- **ECC CPU card Version 1.2 running on SLE77CLFX2407PM (M7794).**

5. The Developer was Gemalto.

6. The TOE is an Electronic Purse (EP) product developed by Gemalto. The TOE operates in an Electronic Money (EM) system to allow the Purseholder to make EM payments securely.

7. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

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

Protection Profile Conformance

9. The ST-lite [ST_LITE] does not claim conformance to any Protection Profile (PP). The ST-lite does not include any additional objectives or Security Functional Requirements (SFRs).

Security Target

10. The ST-lite [ST_LITE] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which these Objectives counter / meet and the SFRs that refine the Objectives. All of the SFRs are taken from CC Part 2 [CC2]; use of that standard facilitates comparison with other evaluated products.

11. All threats to the TOE are countered. The TOE security policies are detailed in the ST-lite [ST_LITE]. The OSPs that must be met are specified in [ST_LITE] Section 4.3

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

Cryptographic Mechanisms

13. The AES cryptographic mechanism contained in the TOE used for data encryption is publicly known and as such it is the policy of CESG, as the UK National Technical Authority for cryptographic mechanisms, not to comment on its appropriateness or strength. However, the Evaluators confirmed its correct implementation.

Evaluation Conduct

14. 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].

15. The evaluators' testing of the TOE was performed at UL's premises in Basingstoke, UK, with final samples.

16. As agreed in advance with the CESG Certification Body, this evaluation reused the site visit results from a previous evaluation (under the French CC Scheme) and no additional site visit was performed during this evaluation.

17. 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-lite [ST_LITE].

18. The results of that work, completed in September 2014, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

19. The TOE should be used in accordance with the environmental assumptions specified in the ST-lite [ST_LITE].

20. 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 (including the 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.

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 that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the TOE document detailed below:

- [AGD] Section 5.4 describes the procedures for identification of the TOE.

32. No other specific security procedures are defined.

Guidance Documents

33. The User Guide and Administration Guide documentation is as follows:

- “AGD: GUIDANCE DOCUMENTS” [AGD].

III. EVALUATED CONFIGURATION

TOE Identification

34. The TOE is ECC CPU card Version 1.2, which consists of Applet (Label R0A23251_EasyCardApplet_VLR) and a Javacard card Platform, GFCX6_EC (Label GFCX6_EC_Cod01_LBL03) running on an already certified Integrated Circuit SLE77CLFX2407PM (M7794).

TOE Documentation

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

TOE Scope

36. The TOE Scope is defined in the ST-lite [ST_LITE] Section 2.3.

37. The TOE is delivered at the end of phase 4, so card embedding (phase 5), personalisation (phase 6) and final usage (phase 7) occur after delivery.

TOE Configuration

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

Environmental Requirements

39. The environmental assumptions for the TOE are stated in the ST-lite [ST_LITE] Section 4.4.

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

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.

43. The TOE is an Electronic Purse (EP) product developed by Gemalto.

44. The TOE operates in an Electronic Money (EM) system, which is able to:

- Store its amount of EM which defines the balance of the EP.
- Indicate amount of EM via Read Purse command.
- Debit its amount of EM via Debit Purse command.
- Credit its amount of EM via Credit Purse command.
- Update parameters via Put Data command.

45. The ECC CPU card primary functionality is to allow the Purseholder to make EM payment in a simple, secure and fast way. The ECC CPU card services are:

- EM protection in term of integrity during Credit, Auto-Load and Debit operations.
- Security assets protection in term of integrity and confidentiality when used or stored.
- Mutual authentication between the TOE and the ECC SAM card during Auto-Load and Debit operations.
- Mutual authentication between the TOE and the Host device during Credit operations.
- Invalidation (i.e. de-activation) of the card via Write Lock command.
- File management commands.

Product Description and Architecture

46. The TOE architecture consists of the following elements, as shown in Figure 1 below.

47. The TOE is a composite product composed of the ECC CPU card Applet running on the GFCX6_EC Javacard Platform in composition with the already certified M7794 IC from Infineon Technologies. The Applet and the Javacard Platform have been developed by Gemalto.

48. The TOE is delivered after phase 5 in closed configuration, meaning that no applets can be loaded.

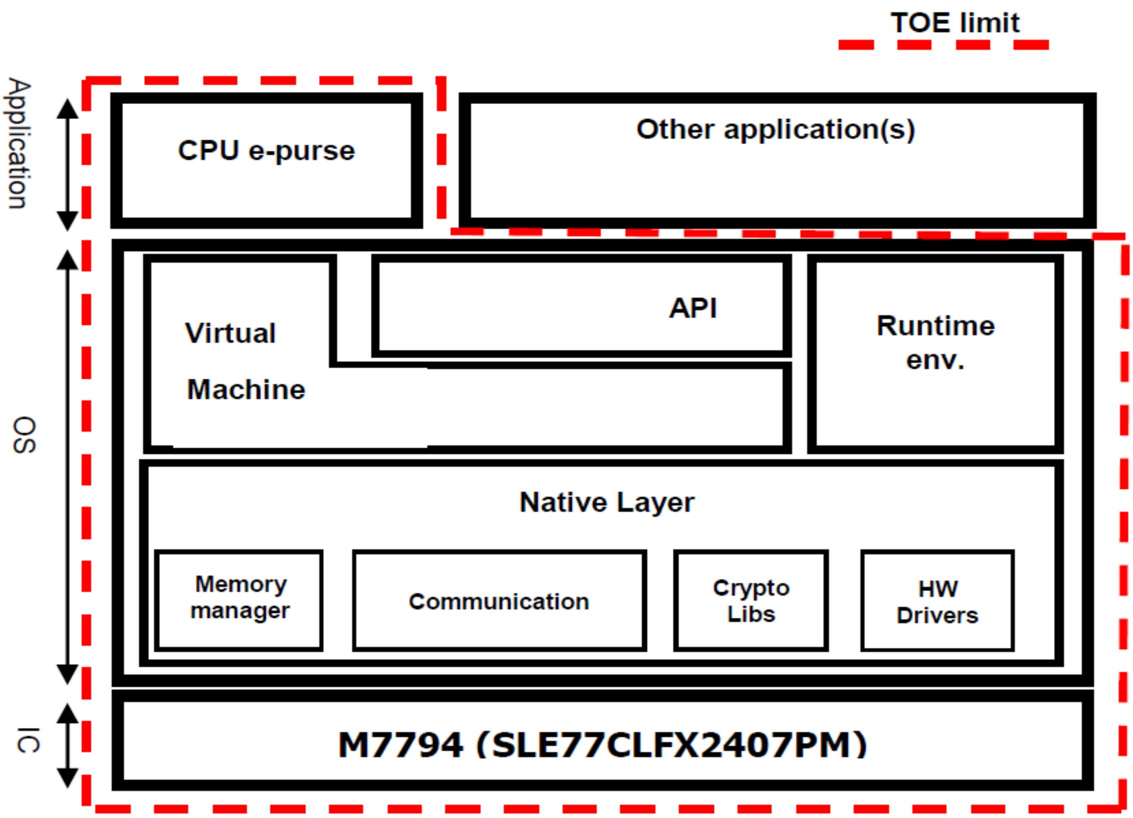

Figure 1 TOE architecture

TOE Design Subsystems

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

- Already certified secure microcontroller.
- Javacard Platform, which provides a secure execution environment for the Applet, including the Card Manager, the Cryptographic library, the Virtual Machine, the low-level code interfacing with the IC, etc.
- The CPU card which provides the core functionality of the applet and support for all the commands available.

TOE Dependencies

50. The TOE has no dependencies.

TOE Security Functionality Interfaces

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

- APDU commands supported by the TOE in phases 6 and 7 are described in the TOE operational guidance [AGD].

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 and a recording of the execution of another sample of these tests.

54. The developer has tested the APDU in the Applet directly. Internal functionality of the Javacard Platform is tested with the use of an emulator.

Evaluator Testing

55. The Evaluators devised and ran 3 independent security functional tests, different from those performed by the Developer. No anomalies were found.

56. The Evaluators also devised and ran 5 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 27th 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 Applet.

59. During the vulnerability analysis, a number of potential vulnerabilities were hypothesised and 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 it does not run on any Platform which is part of the environment.

VI. REFERENCES

[AGD] AGD: GUIDANCE DOCUMENTS,
Gemalto,
R0R23928_CCD_AGD_006, Issue 1.0.

[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,
May 2000.

[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 Transaction Security CLEF,
LFU/T007/ETR, Issue 1.1, 29 September 2014.

[JIL_AM] Attack Methods for Smartcards and Similar Devices,
Joint Interpretation Library,
Version 2.0, February 2011.

[JIL_AP] Application of Attack Potential to Smartcards,
Joint Interpretation Library,
Version 2.8, January 2012.

[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).
[ST]	Security Target for ECC CPU card, Gemalto, R0R23928_CCD_ASE_001, Issue 1.3.
[ST_LITE]	Security Target Lite for ECC CPU card, Gemalto, R0R23928_CCD_ASE_002, Issue 1.3p.
[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, September 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].

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CEN	Comité Européen de Normalisation - European Committee for Standardization
CLEF	Commercial Evaluation Facility
CWA	CEN Workshop Agreement
IC	Integrated Circuit
JIL	Joint Interpretation Library

VII. CERTIFICATE

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

CESG CERTIFICATION BODY

CERTIFICATE No.
P277

This Certificate confirms that

Gemalto ECC CPU card Version 1.2

running on SLE77CLFX2407PM (M7794)

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 and AVA_VAN.5
COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL.

The scope of the evaluated functionality was as claimed by the Security Target and as confirmed by the associated Certification Report **CRP277**.

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

AUTHORISATION
Director for Information Assurance

DATE
19th October 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 ***EN 45011:1998 (ISO/IEC Guide 65:1996)*** 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 EAL4, i.e. the augmentations (AVA_VAN.5 and 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 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 ***EN 45011:1998 (ISO/IEC Guide 65:1996)***, 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.

This page is intentionally blank.