122

CERTIFICATION REPORT No. CRP280

SkySIM CX Hercules

Version 2.0

running on ST33G1M2 Rev. F

Issue 1.0

February 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) [CC] requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.

Sponsor	Giesecke & Devrient GmbH	Developer	Giesecke & Devrient GmbH
Product, Version	SkySIM CX Hercules v2.0		
Integrated Circuit	ST Microelectronics ST33G1M2 Rev F. Certificate: ANSSI-CC-2014/46		
Description	(U)SIM Java Card Open Platform		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP Conformance	(U)SIM Java Card Platform Protection Profile – Basic Configuration v2.0.2		
EAL	EAL4 augmented by ALC_DVS.2 and AVA_VAN.5		
CLEF	UL Transaction Security		
CC Certificate	P280	Date Certified	19 February 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 (U)SIM Java Card Platform Protection Profile (PP) [USIM_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 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

CERTIFICATION STATEMENT **2**

TABLE OF CONTENTS **3**

I. EXECUTIVE SUMMARY **4**

Introduction 4
Evaluated Product and TOE Scope 4
Protection Profile Conformance 4
Security Target 5
Evaluation Conduct 5
Evaluated Configuration 6
Conclusions 6
Recommendations 6
Disclaimers 6

II. TOE SECURITY GUIDANCE **8**

Introduction 8
Delivery and Installation 8
Guidance Documents 8

III. EVALUATED CONFIGURATION **9**

TOE Identification 9
TOE Documentation 9
TOE Scope 9
TOE Configuration 9
Environmental Requirements 9
Test Configurations 9

IV. PRODUCT ARCHITECTURE **10**

Introduction 10
Product Description and Architecture 10
TOE Design Subsystems 10
TOE Dependencies 11
TOE Security Functionality Interfaces 11

V. TOE TESTING **12**

Developer Testing 12
Evaluator Testing 12
Vulnerability Analysis 12
Platform Issues 13

VI. REFERENCES **14**

VII. ABBREVIATIONS **17**

VII. CERTIFICATE **18**

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of SkySIM CX Hercules v2.0 to the Sponsor, Giesecke & Devrient GmbH, 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 SkySIM CX Hercules v2.0, the ST is [ST] and the ST-Lite is [ST_LITE].

3. Prospective consumers of SkySIM CX Hercules v2.0 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 February 2015:

   - **SkySIM CX Hercules Version 2.0 running on ST33G1M2 Rev. F**

5. The Developer was Giesecke & Devrient.

6. The TOE is a (U)SIM Java Card Open Platform in Basic configuration according to [USIM_PP].

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

Protection Profile Conformance

10. The ST [ST]/[ST_LITE] is certified as achieving conformance to the (U)SIM Java Card Platform Protection Profile – Basic Configuration v2.0.2.

Security Target

11. The ST [ST]/[ST_LITE] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which these Objectives counter / meet and the Security Functional Requirements (SFRs) that refine the Objectives.

12. All threats to the TOE are countered.

13. The TOE security policies are detailed in ST [ST]/[ST_LITE] .

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

15. Most of the SFRs in the ST [ST]/[ST_LITE] are taken from the PP [USIM_PP] which facilitates comparison with other evaluated products.

16. The ST [ST]/[ST_LITE] also include Complementary Security Objectives for the TOE and Additional SFRs, which were objectives for the environment in [USIM_PP], namely OE.SCP.RECOVERY, OE.SCP.SUPPORT and OE.SCP.IC.

17. The OSPs that must be met are specified in [ST]/[ST_LITE] Section 4.4.

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

Evaluation Conduct

19. 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) [JIL] has been used. The applicable documentation is the following:

    - 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].
    - Certification of "open" smart card products [NOTE10].

20. The testing of the TOE has been done entirely at UL's premises in Basingstoke, UK, with final samples.

21. No site visit has been performed during this evaluation. The site visit results from the site certificates under the German Scheme have been reused.

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 ST [ST]/[ST_LITE]. The results of this work, completed in February 2015, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

23. 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.

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 61).

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 that is of particular relevance to consumers of the TOE.

Delivery and Installation

34. 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 2.1.3 of [PERSO_GUIDE] describes the procedures for identification of the TOE.

35. No other specific security procedures are defined.

Guidance Documents

36. The guidance documentation is as follows:

- [DEV_GUIDE]
- [AP_GUIDE]
- [CA_GUIDE]
- [MNO_GUIDE]
- [PERSO_GUIDE]
- [TERMINAL_GUIDE]
- [COMMON_GUIDE]
- [VA_GUIDE]
- [INIT_GUIDE]

III. EVALUATED CONFIGURATION

TOE Identification

37. The TOE is SkySIM CX Hercules v2.0, which consists of the embedded software in composition with the already certified ST33G1M2 Rev. F security IC from ST Microelectronics [CR_IC].

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 ST [ST]/[ST_LITE] Section 1.5. The TOE is delivered at the end of phase 4, so Composite Product Integration (phase 5), Personalization (phase 6) and Final Usage (phase 7) occur after this delivery.

TOE Configuration

40. 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]/[ST_LITE] Section 5.2.

42. The TOE relies on the off-card bytecode verifier to operate securely in Final Usage (OE.Verification).

Test Configurations

43. There are no different configurations other than the one defined in ST [ST]/[ST_LITE].

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 (U)SIM Java Card platform embedded in a (U)SIM card - a (U)SIM Java Card Platform in Basic configuration as defined in [USIM_PP]. It is intended to be plugged in a mobile phone or other mobile device. The TOE consists of the related embedded software and firmware in combination with the underlying hardware and offers the following security features:

- Security services to Applets through the available APIs.
- Confidentiality and integrity of Application secrets, data and code.
- Card content management as specified in Global Platform [GP].

46. The TOE is composed of:

- the circuitry of the ST33G1M2 Rev. F Secure Microcontroller;
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
- the OS, Java Card System and Issuer Security Domain (ISD), Supplementary Security Domain (SSD) applets;
- the associated guidance documentation.

Product Description and Architecture

47. The TOE is a composite product composed of the OS, Java Card System and ISD, SSD applets running in composition with the already certified ST33G1M2 Rev. F Secure Microcontroller from ST Microelectronics [CR_IC]. The embedded software has been developed by Giesecke & Devrient.

TOE Design Subsystems

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

APDU

49. This subsystem is the entry point of APDU commands sent to the TOE. It implements the APDU handling (T=0, SWP, logical channels) and the Issuer Security Domain.

Telco Sys

50. This subsystem implements all the telecommunication features. It contains the application dispatcher for the telco APDUs and also implements the Telco API available to applications, such as access to SIM and USIM file systems, registration of events of the application toolkit framework, network authentication and OTA services.

API

51. This subsystem implements the Javacard, GP, USIM and UICC APIs that are available to applets.

JCVM

52. This subsystem implements the Javacard Virtual Machine in charge of interpreting the bytecode, handling java exceptions and performing the firewall checks. It also implements Memory Management functions needed by the JCVM.

Hardware

53. This subsystem represents the ST33G1M2 Rev. F Secure Microcontroller, which has been certified EAL5 augmented by ALC_DVS.2 and AVA_VAN.5. (Refer to [CR_IC].)

TOE Dependencies

54. The TOE has no dependencies.

TOE Security Functionality Interfaces

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

- APDU commands for Card Content Management,
- APIs (Java Card, Global Platform, USIM and UICC),
- Bytecodes – interface with the JCVM Virtual Machine,
- Electrical interface (reset, power supply).

V. TOE TESTING

Developer Testing

56. 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.

57. 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.

58. The developer has tested the TSFI directly in the final TOE. Internal functionality of the TOE is tested with the use of dedicated test tools.

Evaluator Testing

59. The Evaluators devised and ran a total of 9 independent security functional tests, different from those performed by the Developer. No anomalies were found.

60. The Evaluators also devised and ran a total of 26 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

61. The Evaluators completed their penetration tests in October 2014.

Vulnerability Analysis

62. 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.

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

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

Platform Issues

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

VI. REFERENCES

[AP_GUIDE] Class AGD_OPE: Operational User Guidance for the Application Provider - SkySIM CX Hercules v2.0,
Version 1.1.

[CA_GUIDE] Class AGD_OPE: Operational User Guidance for the Controlling Authority - SkySIM CX Hercules v2.0,
Version 1.0.

[COMMON_GUIDE] Class AGD_OPE: Operational User Guidance Common Document - SkySIM CX Hercules v2.0,
Version 1.1.

[DEV_GUIDE] Class AGD_OPE: Operational User Guidance for the Application Developer - SkySIM CX Hercules v2.0,
Version 1.1.

[INIT_GUIDE] Initialization Guidance SkySIM CX Hercules v2.0,
Version 1.2.

[MNO_GUIDE] Class AGD_OPE: Operational User Guidance for the Mobile Network Operator - SkySIM CX Hercules v2.0,
Version 1.1.

[PERSO_GUIDE] Class AGD_OPE: Operational User Guidance for the Personaliser - SkySIM CX Hercules v2.0,
Version 1.0.

[TERMINAL_GUIDE] Class AGD_OPE: Operational User Guidance for the Terminal - SkySIM CX Hercules v2.0,
Version 1.0.

[VA_GUIDE] Class AGD_OPE: Operational User Guidance for the Verification Authority - SkySIM CX Hercules v2.0,
Version 1.1.

[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_IC] Certification Report ANSSI-CC-2014/46 – ST33G1M2 Secure microcontroller revision F, Firmware revision 9, with optional NesLib 4.1 cryptographic library and MIFARE® DESFire® EV1 library revision 3.7 or 3.8,
21st July 2014.

[ETR] Evaluation Technical Report,
UL Transaction Security CLEF,
LFU/T008/ETR, Issue 1.0, January 2015.

[GP] GlobalPlatform Card Specification
Version 2.2.1, January 2011.

[JIL] Joint Interpretation Library,
(comprising [JIL_AM], [JIL_AP], [JIL_ARC], [JIL_COMP] and [NOTE_10]).

[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).

[NOTE10] Certification of "open" smart card products,
Version 1.1 (for trial use), 4th February 2013.

[USIM_PP] (U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations,
Version 2.0.2, 17th June 2010.

[ST] SkySIM CX Hercules v2.0 Security Target,
Version 1.7, 2014-12-17.

[ST_LITE] SkySIM CX Hercules v2.0 Security Target Lite,
Version 1.0, 2014-12-18.

[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].

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
GP	Global Platform
IC	Integrated Circuit
ISD	Issuer Security Domain
JIL	Joint Interpretation Library
SIM	Subscriber Identity Module
SSD	Supplementary Security Domain
SWP	Single Wire Protocol
USIM	Universal Subscriber Identity Module
UICC	Universal Integrated Circuit Card

VII. CERTIFICATE

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

CESG CERTIFICATION BODY

CERTIFICATE No.
P280

This Certificate confirms that

Giesecke & Devrient GmbH – SkySIM CX Hercules v2.0

running on ST33G1M2 Rev. F

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
and (U)SIM Java Card Platform Protection Profile
– Basic Configuration v2.0.2

The scope of the evaluated functionality was as claimed by the Security Target
and as confirmed by the associated Certification Report **CRP280**.

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
19 February 2015

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.

Standards: Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7.

Details are provided on the UKAS website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), 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 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 ***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.

This page is intentionally left blank