0122

Common Criteria Certification Report

No. CRP299

SkySIM CX Hercules M4M

Version 1.0
running on ST33G1M2 Rev. F

Issue 1.0

March 2017

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	Giesecke & Devrient GmbH	Developer	Giesecke & Devrient GmbH
Product Name, Version	SkySIM CX Hercules M4M Version 1.0		
Platform/Integrated Circuit	ST33G1M2 Rev. F		
Description	(U)SIM Java Card platform		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(s) or (c)PP Conformance	(U)SIM Java Card™ Platform Protection Profile- Basic configuration Version 2.0.2 Java Card™ System Open Configuration Version 3.0		
EAL	CC EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5		
CLEF	UL Transaction Security		
CC Certificate	P299	Date Certified	31 March 2017

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 [UKSP01]. 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], 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 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.

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] recognition for components up to EAL 2 only, i.e. all other components, including the augmentations ALC_DVS.2 and AVA_VAN.5, are not covered by the CCRA. All judgements in this Certification Report are covered by the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the above product at the stated version, to the Sponsor 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. Prospective consumers of the above product at the stated version should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]/[ST-Lite], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product(s) completed evaluation to CC EAL4 assurance level augmented by ALC_DVS.2 and AVA_VAN.5 on 31 March 2017:

SkySIM CX Hercules M4M Version 1.0 running on ST33G1M2 Rev. F

4. The Developer was Giesecke & Devrient GmbH.

5. The Target of Evaluation (TOE) is a (U)SIM Java Card platform embedded in a (U)SIM card 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.

6. 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 'Evaluation Configuration' of this report.

7. The TOE depends on the secure operational environment that includes the off-card bytecode verifier.

8. An overview of the TOE and its product architecture can be found in Chapter IV 'TOE Architecture' of this report. Configuration requirements are specified in Section 1.4 of the Security Target [ST]/[ST-Lite].

Protection Profile Conformance

9. The Security Target [ST]/[ST-Lite] is certified as achieving conformance to the following protection profiles:

   - (U)SIM Java Card™ Platform Protection Profile - Basic configuration Version 2.0.2 [PP(U)SIM].
   - Java Card™ System Open Configuration Version 3.0 [PPJCSv3.0].

10. The ST also includes security objectives, security assurance requirements and Security Functional Requirements (SFRs) additional to those of the Protection Profiles.

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 counter or meet and the Security Functional Requirements (SFRs) that refine the Objectives. Most of the SFRs are taken from [PP(U)SIM], which is based on [PPJCSv3.0], which in turn takes them from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

12. The assurance requirements are taken from CC Part 3 [CC3].

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

14. The cryptographic algorithms are specified in Section 7 of [ST]/[ST-Lite]. These are consistent with the recognised, agreed cryptographic mechanisms detailed in [CWG_MECHS].

Evaluation Conduct

15. The evaluation used the CCRA supporting documents as appropriate, SOGIS supporting documents defined in [JIL], international interpretations together with the relevant UK interpretations.

16. The JavaCard Platform source code was reviewed in UL's premises in Basingstoke (UK).

17. The Evaluator's independent security functional tests, and the repeat of a sample of the Developer's tests overseen by the Evaluator, were performed in G&D's premises in Barcelona.

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

19. The site visit results from previous evaluations were reused, as detailed in the Evaluation Technical Report [ETR].

20. The CESG Certification Body monitored the evaluation, which was performed by the UL Transaction Security Commercial Evaluation Facility (CLEF), and witnessed a sample of Evaluator tests. The evaluation addressed the requirements specified in the Security Target [ST]/[ST-Lite]. The results of this work, completed in March 2017, were reported in the Evaluation Technical Report(s) [ETR].

Evaluated Configuration

21. 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.

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

Conclusions

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

Recommendations

24. 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.

25. The TOE relies on the Crypto Libraries and Security Mechanisms of the IC. System integrators and risk owners using the TOE should therefore make suitable arrangements to satisfy themselves that they have appropriate confidence in the mechanisms of the IC, in particular any patches or updates.

26. Any further recommendations are included in the TOE Security Guidance in Chapter II, Paragraph 40.

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 'Evaluation 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 63).

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 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(s) detailed below:

    - Section 3 of [UG_PRE].

Guidance Documents

35. Specific configuration advice is included in the smart card guidance documents listed in this section.

36. The User Guide and Administration Guide documentation is in the smart card guidance listed below.

37. The guidance documentation for the Pre-personalization phase is as follows:

    - [UG_PRE] Preparative Procedures.

38. The guidance documentation for the Personalization phase is as follows:

    - [UG_OPE_PERSO] Operational User Guidance for the Personaliser;
    - [UG_OPE] Operational User Guidance Common Document.

39. The guidance documentation for the Operational phase is as follows:

    - [UG_OPE] Operational User Guidance Common Document;
    - [UG_OPE_AD] Operational User Guidance for the Application Developer;
    - [UG_OPE_AP] Operational User Guidance for the Application Provider;
    - [UG_OPE_CA] Operational User Guidance for the Controlling Authority;
    - [UG_OPE_MNO] Operational User Guidance for the Mobile Network Operator;

- [UG_OPE_TERM] Operational User Guidance for the Terminal;
- [UG_OPE_VA] Operational User Guidance for the Verification Authority.

Recommendations

40. To maintain secure operation, the consumer is recommended to follow the smart card guidance detailed in the documentation listed above.

III. EVALUATED CONFIGURATION

TOE Identification

41. The TOE is SkySIM CX Hercules M4M Version 1.0, which consists of a (U)SIM Java Card platform in composition with the certified underlying IC ST33G1M2 Rev. F.

TOE Documentation

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

TOE Scope

43. The TOE Scope is defined in the Security Target ([ST]/[ST-Lite]) Section 1.4.6. Functionality that is outside the TOE Scope is defined in Section 1.4.7.

TOE Configuration

44. The evaluated configuration of the TOE is defined in the Security Target Section 1.4.1 and specific configuration advice is provided in the Evaluated Configuration Guide [UG_PRE].

45. The evaluated TOE configuration is composed of:

- ST33G1M2 Rev. F;
- SkySIM CX Hercules OS;
- Java Card Platform 3.0.4;
- Native Telecommunication Application.

Environmental Requirements

46. The environmental objectives for the TOE are stated in Section 5.2 of [ST]/[ST-Lite].

47. The environmental assumptions for the TOE are stated in Section 4.5 of [ST]/[ST-Lite].

Test Configurations

48. The Developers and Evaluators used different variants of the SkySIM CX Hercules M4M Version 1.0 Java Card Open Platform code during evaluation and testing. However, the Evaluator's independent results derived from vulnerability analysis and code comparison demonstrated that the test configurations were all consistent with the TOE configuration as defined in Paragraph **Error! Reference source not found.** above.

IV. TOE ARCHITECTURE

Introduction

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

TOE Description and Architecture

50. The TOE is a (U)SIM Java Card platform in composition with the certified underlying IC ST33G1M2 Rev. F [IC_CR], as described in Section 1.4.2 of [ST]/[ST-Lite].

51. The TOE is composed of the following security components:

- A Java Card System as defined in [PPJCSv3.0], including all the native code, which manages and executes applications called applets. It provides APIs for developing applets in accordance with the Java Card specification, [JCAPI304];
- GlobalPlatform (GP) packages providing a common interface to communicate with a smart card and manage applications in a secure way according to the [GP] specifications;
- (U)SIM APIs for interacting with (U)SIM applications, according to [TS131 130] specifications;
- The SCP (Smart Card Platform) comprises the IC (Integrated Circuit) and the OS (Operating System).

	TOE of the PP	SkySIM CX Hercules TOE
①	The Smart Card Platform (SCP) is a combination of the Integrated Circuit (IC) and the native Operating System (OS).	ST33G1M2 Rev. F and SkySIM CX Hercules OS
②	Java Card System (JCRE, JCVM, JCAPI)	Java Card Platform 3.0.4 classic implementation
③	Additional native code, proprietary applications	Native Telecommunication Application
④	Applets	The TOE does not include applets.

Table 1 - Correspondence of TOE building blocks in the Protection Profiles and in [ST]

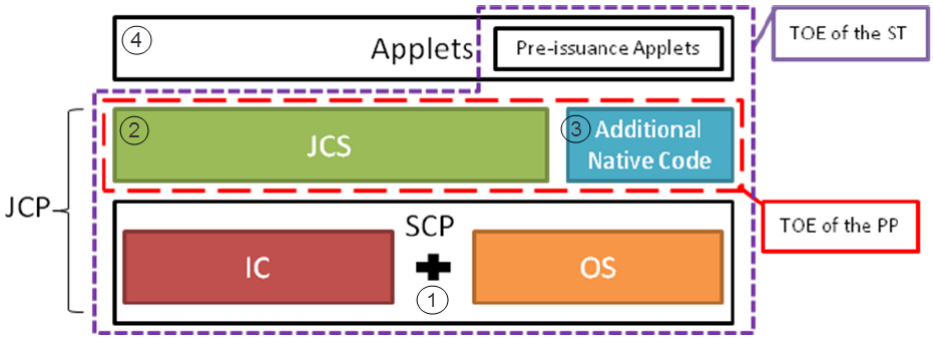

Figure 1 - Java Card Platform TOE boundaries defined in [PPJCSv3.0]

52. The following GP functionality is present within the TOE:

- Card and Application management according to [GP]:
  - Content loading, installation, making selectable, removal, extradition;
  - DAP verification and mandated DAP verification;
  - Security Domain and application privileges.
- Secure Channel protocols (SCP02, SCP03 and SCP80);
- Support for contactless cards (ATQ, different implicit selection on different interfaces and channels) and GP CL API;
- Post-issuance personalization of Security Domain;
- Application personalisation.

53. The TOE supports the cryptographic algorithms AES, TDES, RSA and ECC.

TOE Design Subsystems

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

- APDU: this subsystem is the entry point of APDU commands sent to the TOE. It implements the APDU handling (and the Issuer Security Domain.
- API: this subsystem implements the Java Card APIs [JCAPI304] and GlobalPlatform APIs [GP] that are available to applets, plus the UICC and USIM APIs according to [ETSI_TS_102_241], [ETSI_TS_102_705] and [ETSI_TS_131_130]. G&D proprietary APIs are also part of this subsystem.
- VM: this subsystem implements the Java Card Virtual Machine (JCVM), the bytecode interpreter in charge of interpreting the bytecodes according to [JCVM304], handling java exceptions and performing the firewall checks. It also implements Memory Management functions according to [JCRE304] needed by the JCVM.

- TELCO_SYS: this subsystem implements the telecommunication related features.

- HW: this subsystem implements the TOE hardware platform, the ST33G1M2 Rev. F security IC, which is certified to CC EAL5 augmented by ALC_DVS.2 and AVA_VAN.5 [IC_CR].

TOE Dependencies

55. The TOE has no dependencies.

TOE Security Functionality Interface

56. The external TOE Security Functionality Interface (TSFI) is:

- APDU commands;

- APIs (Java Card, GlobalPlatform and proprietary APIs);

- Bytecodes (interface with the JCVM);

- Electrical interface (reset, power supply).

V. TOE TESTING

Developer Testing

57. 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.

58. 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/repeated a sample of the Developer's security tests.

59. The Developer security tests, which included both black box and white box testing, were run on the configuration defined in Chapter III 'Test Configurations'.

Evaluator Testing

60. The Evaluators devised and ran a total of 16 independent security functional tests, different from those performed by the Developer. No anomalies were found.

61. The Evaluators also devised and ran a total of 24 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

62. The Evaluators ran their tests on the configuration defined in Chapter III 'Test Configurations'.

63. The Evaluators completed their penetration tests on 26 August 2016.

Vulnerability Analysis

64. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables. The analysis of the evaluation deliverables followed the SOG-IS guidance provided in the [JIL] documentation.

Platform Issues

65. The platform relevant to the TOE is detailed in Chapter III and no platform issues were identified.

VI. REFERENCES

[CC]	Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2] and [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.
[CWG_MECHS]	Agreed Cryptographic Mechanisms, SOG-IS Crypto Working Group, V1.0, May 2016
[ETR]	Evaluation Technical Report, UL CLEF, LFU/T022/ETR, Issue 1.0, March 2017.
[ETSI_TS_102_241]	Smart Cards; UICC Application Programming Interface (UICC API) for Java Card™ (Release 9), ETSI TS 102 241, V9.2.0, March 2012

[ETSI_TS_102_705]	ETSI TS 102 705 V10.0.0 (2011-09), UICC Application Programming Interface for Java Card for Contactless Applications, ETSI TS 102 705, V10.0.0, September 2009
[ETSI_TS_131_130]	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; (U)SIM Application Programming Interface (API); (U)SIM API for Java™ Card (3GPP TS 31.130 version 11.0.0 Release 11), ETSI TS 131 130, V11.0.0, April 2013
[GP]	GlobalPlatform Card Specification, GlobalPlatform Inc, Version 2.2.1, January 2011.
[IC_CR]	Rapport de maintenance, ANSSI, ANSSI-CC-2014/46-M01, issue 2016-03-17.
[JCAPI304]	Java Card ™ API, Classic Edition, Oracle, E18985-01, Issue 3.0.4, September 2011
[JCRE304]	Java Card 3 Platform – Runtime Environment Specification, Classic Edition, Oracle, E18985-01, Version 3.0.4, September 2011.
[JCVM304]	Java Card 3 Platform – Virtual Machine Specification, Classic Edition, Oracle, E25256-01, Version 3.0.4, September 2011.
[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 1.4, August 2015.
[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.
[PP(U)SIM]	Common Criteria Protection Profile, (U)SIM Java Card Platform, Basic and SCWS Configurations, Evolutive Certification Scheme for (U)SIM cards, Version 2.0.2, 17 June 2010 PU-2009-RT-79
[PPJCSv3.0]	Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 ANSSI-CC-PP-2010/03
[TS131 130]	ETSI TS 131 130 V11.0.0 (2013-04), Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; (U)SIM Application Programming Interface (API); (U)SIM API for Java™ Card (3GPP TS 31.130 version 11.0.0 Release 11)
[ST]	Security Target, Giesecke & Devrient GmbH, ST_2016-12-22, Issue 2.1, December 2016.
[ST-Lite]	Security Target Lite, Giesecke & Devrient GmbH, ST-LITE_2016-12-22, Issue 2.1, December 2016.
[UG_OPE]	SkySIM CX Hercules M4M Operational Guidance Common Document, Giesecke & Devrient GmbH, Issue 1.6, 08/11/2016.

[UG_OPE_AD]	SkySIM CX Hercules M4M Operational Guidance for the Application Developer, Giesecke & Devrient GmbH, Issue 1.1, 22/11/2016.
[UG_OPE_AP]	SkySIM CX Hercules M4M Operational Guidance for the Application Provider, Giesecke & Devrient GmbH, Issue 1.0, 14/03/2016.
[UG_OPE_CA]	SkySIM CX Hercules M4M Operational Guidance for the Controlling Authority, Giesecke & Devrient GmbH, Issue 1.0, 14/03/2016.
[UG_OPE_MNO]	SkySIM CX Hercules M4M Operational Guidance for the Mobile Network Operator, Giesecke & Devrient GmbH, Issue 1.1, 18/10/2016.
[UG_OPE_PERSO]	SkySIM CX Hercules M4M Operational Guidance for Personaliser, Giesecke & Devrient GmbH, Issue 1.1, 20/09/2016.
[UG_OPE_TERM]	SkySIM CX Hercules M4M Operational Guidance for the Terminal, Giesecke & Devrient GmbH, Issue 1.0, 14/03/2016.
[UG_OPE_VA]	SkySIM CX Hercules M4M Operational Guidance for the Verification Authority, Giesecke & Devrient GmbH, Issue 1.0, 14/03/2016.
[UG_PRE]	SkySIM CX Hercules M4M Preparative Procedures, Giesecke & Devrient GmbH, Issue 1.4, 18/10/2016.
[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.

Standard CC abbreviations are detailed in CC Part 1 [CC1] and UK Scheme abbreviations and acronyms are detailed in [UKSP00].

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
GP	GlobalPlatform
IC	Integrated Circuit
JCAPI	Java Card Application Programming Interface
JCRE	Java Card Runtime Environment
JCS	Java Card System
JCVM	Java Card Virtual Machine
JIL	Joint Interpretation Library
LFU	CLEF UL
MAC	Message Authentication Code
OS	Operating System
RSA	Rivest Shamir Adleman
TDES	Triple DES
UL	Underwriters Laboratories Inc.
USIM	Universal Subscriber Identity Module
VA	Vulnerability Analysis
VM	Virtual Machine

VIII. CERTIFICATE

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

CESG Certified Product

Common Criteria

P299

This is to certify that

Giesecke & Devrient GmbH

SkySIM CX Hercules M4M

Version 1.0

Running on ST33G1M2 Rev. F

has been evaluated under the terms of the

Common Criteria Scheme

and complies with the requirements for

(U)SIM Java Card™ Platform Protection Profile- Basic configuration Version 2.0.2
Java Card™ System Open Configuration Version 3.0

Common Criteria

UKAS PRODUCT CERTIFICATION

SOGIS IT SECURITY CERTIFIED

AUTHORISED BY
DIRECTOR GENERAL
FOR GOVERNMENT
AND INDUSTRY CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
UL Transaction Security

DATE AWARDED
31 March 2017

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ISO/IEC17065:2012 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)

The IT Product identified in this certificate has been evaluated at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification/Validation Report for conformance to the Common Criteria for IT Security Evaluation, version 3.1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the Common Criteria Scheme and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

All judgements contained in this certificate, and in the associated Certification Report, are covered by CCRA recognition for components up to EAL2 only, i.e., all other components, including 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 judgements contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issues them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgements or for loss sustained as a result of reliance upon those judgements by a third party.
All judgements contained in this certificate, and in the associated Certification Report, are covered by the agreement.

In conformance with the requirements of ***ISO/IEC17065:2012***, the CCRA and the SOGIS MRA, the Common Criteria website (http://www.commoncriteriaportal.org) 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).