



0122

# Common Criteria Certification Report

No. CRP300

**SkySIM CX Virgo**

**Version 3.0**  
running on Broadcom BCM\_SPS02 C0

Issue 1.0  
April 2017

© Crown Copyright 2016 – All Rights Reserved

Reproduction is authorised, provided  
that this report is copied in its entirety

**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 Virgo Version 3.0		
Platform/Integrated Circuit	Broadcom BCM_SPS02 C0 [CR_IC], [CR_IC_MR]		
Description	Embedded Secure Element with Java Card Open Platform		
CC Version	Version 3.1 Release 4		
CC Part 2	Conformant	CC Part 3	Conformant
PP(s) or (c)PP Conformance	Java Card Protection Profile, Open Configuration, Version 3.0, May 2012 [PP]		
EAL	CC EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5		
CLEF	UL Transaction Security		
CC Certificate	P300	Date Certified	21 April 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 [UKSP02]. 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 [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<sup>1</sup> 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<sup>1</sup> 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.



<sup>1</sup> 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**

**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

Recommendations ..... 8

**III. EVALUATED CONFIGURATION .....9**

TOE Identification ..... 9

TOE Documentation ..... 9

TOE Scope ..... 9

TOE Configuration ..... 9

Environmental Requirements..... 9

Test Configurations..... 9

**IV. TOE ARCHITECTURE.....10**

Introduction..... 10

TOE Description and Architecture..... 10

TOE Design Subsystems..... 11

TOE Dependencies ..... 12

TOE Security Functionality Interface ..... 12

**V. TOE TESTING.....13**

Developer Testing ..... 13

Evaluator Testing ..... 13

Vulnerability Analysis ..... 13

Platform Issues ..... 14

**VI. REFERENCES .....15**

**VII. ABBREVIATIONS .....19**

**VIII. CERTIFICATE .....20**

---

## 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 completed evaluation to CC EAL4 assurance level augmented by ALC\_DVS.2 and AVA\_VAN.5 on 21 April 2017:

#### **SkySIM CX Virgo Version 3.0 running on Broadcom BCM\_SPS02 C0**

4. The Developer of SkySIM CX Virgo V3.0 is Giesecke & Devrient GmbH.
5. The Target of Evaluation (TOE) is an embedded Secure Element (eSE) intended to be soldered in a mobile phone or other mobile device. The TOE permits customer applets to implement applications such as contactless secure payment and robust identity solutions.
6. The TOE consists of the related embedded software and firmware in combination with the underlying hardware. Further details are provided in Chapter IV 'TOE Architecture'.
7. The evaluated configuration of this product is described as the TOE. Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluation Configuration'.
8. An overview of the TOE and its product architecture can be found in Chapter IV 'TOE Architecture'. 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 demonstrable conformance to the following protection profile:
  - Java Card Protection Profile, Open Configuration, Version 3.0, May 2012 [PP].

10. The ST also includes security objectives, security assurance requirements and Security Functional Requirements (SFRs) from [USIM\_PP], additional to those of the [PP]. Conformance to the [USIM\_PP] is not claimed because the TOE is an Embedded Secure Element and not a (U)SIM card.

### ***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] which in turn takes them from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.
12. Additional SFRs are added into [ST]/[ST-Lite] to cover proprietary features of the TOE; these additional SFRs are taken from CC Part 2 [CC2].
13. The assurance requirements are taken from CC Part 3 [CC3].
14. The OSPs that must be met are specified in Section 5.3.2 of [ST]/[ST-Lite].
15. The environmental objectives and assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements').
16. The cryptographic algorithms implemented in the product are specified in Section 6 of [ST]/[ST-Lite]. These are consistent with the recognised, agreed cryptographic mechanisms detailed in [CWG\_MECHS].

### ***Evaluation Conduct***

17. The evaluation used the following documents as appropriate: the CCRA supporting documents, the SOGIS supporting documents defined in [JIL], international interpretations and relevant UK interpretations.
18. The source code of the Java Card Platform and CRS applet was reviewed in UL's premises in Basingstoke (UK).
19. 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.
20. Penetration testing of the TOE was performed entirely at UL Transaction Security's premises in Basingstoke, UK, using final samples of the TOE. The test approach used the latest advanced techniques, including the attack methods detailed in [JIL\_AM].
21. The site visit results from previous evaluations were reused, as detailed in the Evaluation Technical Report [ETR].

22. 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 December 2016, 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 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.
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 in the 'Certification Statement' on page 2.

### ***Recommendations***

26. Chapter II 'TOE Security Guidance' includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.
27. The TOE utilises the Crypto Libraries and Security Mechanisms of the IC. System integrators and risk owners should make sure they have confidence in the mechanisms of the IC, in particular paying attention to any patches or updates.
28. Any further recommendations are included in the TOE Security Guidance in Chapter II, Paragraph 42.

### ***Disclaimers***

29. 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'. The ETR on which this Certification Report is based relates only to the specific items tested.
30. 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 Chapter V, Paragraph 68).

- 
31. 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.
  32. 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 approach. Unevaluated patches are not covered by this 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.
  33. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.
  34. 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.

---

## II. TOE SECURITY GUIDANCE

### *Introduction*

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

### *Delivery and Installation*

36. 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:

- Sections 2 and 3 of [AG].

### *Guidance Documents*

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

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

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

- [AG] Preparative Procedures.

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

- [UG\_PERSO] Operational User Guidance for the Personaliser;
- [UG\_COMMON] Operational User Guidance Common Document.

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

- [UG\_COMMON] Operational User Guidance Common Document;
- [UG\_AD] Operational User Guidance for the Application Developer;
- [UG\_AP] Operational User Guidance for the Application Provider;
- [UG\_CA] Operational User Guidance for the Controlling Authority;
- [UG\_ISSUER] Operational User Guidance for the Issuer;
- [UG\_VA] Operational User Guidance for the Verification Authority.

### *Recommendations*

42. 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***

43. The TOE is SkySIM CX Virgo Version 3.0, which consists of a Java Card Platform in Open Configuration in composition with the certified underlying IC platform BCM\_SPS02 C0.

#### ***TOE Documentation***

44. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in 'Guidance Documents').

#### ***TOE Scope***

45. The TOE Scope is defined in the Security Target ([ST]/[ST-Lite]) Section 1.4. Functionality that is outside the TOE Scope is defined in Sections 1.4.8 and 1.4.9. The TOE boundaries are shown in Figure 1 below.

#### ***TOE Configuration***

46. The evaluated configuration of the TOE is defined in the Security Target Section 1.4.1 and specific configuration advice is provided in the guidance [UG].
47. The evaluated TOE configuration is composed of:
- SkySIM CX Virgo v3.0 Java Card Open Platform, Code v2.1.2;
  - BCM\_SPS02 C0, Firmware/Bootloader v002.020;
  - CRS applet: Date 20th June 2016, 11:45:35, GIT HASH c88b2fbaf8f9c7d5e54d0eb50a319fc2ef149420.

#### ***Environmental Requirements***

48. The environmental objectives for the TOE are stated in Section 5.2 of [ST]/[ST-Lite].
49. The environmental assumptions for the TOE are stated in Section 4.5 of [ST]/[ST-Lite].

#### ***Test Configurations***

50. The Developers and Evaluators used successive development versions of the SkySIM CX Virgo v3.0 Java Card Open Platform code during evaluation. However, the Evaluator's independent results derived from vulnerability analysis, profiling analysis and comparison tests demonstrated that the test configurations were all consistent with the following configuration:
- The TOE configuration as defined in Paragraph 47 above.

## IV. TOE ARCHITECTURE

### Introduction

51. 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'.

### TOE Description and Architecture

52. The TOE is an embedded Secure Element (eSE), a composite product made of the SkySIM CX Virgo V3.0 Java Card Platform in Open Configuration in composition with the certified BCM\_SPS02 C0 security IC from Broadcom [CR\_IC], as described in Section 1.4.1 of [ST]/[ST-Lite].

53. The TOE is comprised of the following:

- A Java Card System as defined in the [PP], 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 to manage applications in a secure way according to the [GP221] specifications.
- The Smart Card Platform (SCP), comprising the Integrated Circuit (IC) and the Operating System (OS).

	TOE of the PP	SkySIM CX Virgo TOE
①	The Smart Card Platform (SCP) is a combination of the Security Integrated Circuit (IC) and the native Operating System (OS).	BCM_SPS02 C0 and SkySIM CX Virgo OS
②	Java Card System (JCRE, JCVM, JCAPI)	Java Card Platform 3.0.4 classic implementation
③	Additional native code, proprietary applications	Native Applications
④	Applets	The TOE includes only the CRS applet. (Other customer applets are excluded from the TOE scope.)

Table 1: Correspondence of TOE building blocks in [PP] and [ST]

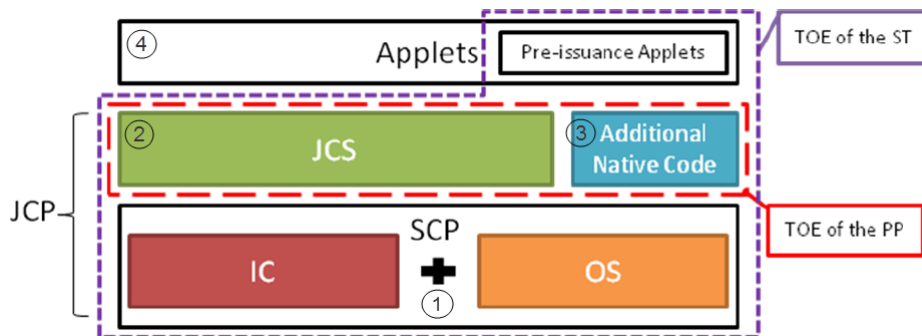


Figure 1: SkySIM Virgo V3.0 TOE boundaries defined in [PP]

54. Since post-issuance installation of applets is possible, the TOE corresponds to an open configuration, as defined in [PP].
55. The TOE 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 in line with the GlobalPlatform specification;
  - OS Update and Applet Migration functionalities;
  - CRS applet.
56. The TOE supports the cryptographic algorithms AES, TDES, RSA, ECDSA, ECDH and MAC Algorithm 3; Secure Channel Protocols 02 and 03 (SCP02 and SCP03) provide confidentiality and integrity.
57. The TOE implements the Single Wire Protocol (SWP) for contactless communication.
58. The TOE also applies masking operations to keys and sensitive data to provide confidentiality of data used by applications running on the eSE.

### **TOE Design Subsystems**

59. 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 (SWP, logical channels) and the Issuer Security Domain.
  - API: this subsystem implements the Java Card APIs [JC-API304] and GlobalPlatform APIs [GP221] that are available to applets.

- 
- 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.
  - HW: this subsystem implements the TOE hardware platform, the Broadcom BCM\_SPS02 C0 security IC, which is certified to CC EAL5 augmented by ALC\_DVS.2 and AVA\_VAN.5 [CR\_IC].

### ***TOE Dependencies***

60. The TOE has no dependencies.

### ***TOE Security Functionality Interface***

61. 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*

62. The Developer's security tests covered:
- all SFRs;
  - all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems');
  - all TOE Security Functionality;
  - the TSFI, as identified in Chapter IV (in 'TOE Security Functionality Interface').
63. 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 the Developer repeating a sample of Developer security tests.
64. 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*

65. The Evaluators devised and ran a total of 6 independent security functional tests, different from those performed by the Developer. No anomalies were found.
66. The Evaluators devised a set of 16 comparison tests based on profiling analysis in order to demonstrate the validity of the penetration testing performed during the evaluation of the previous versions of the product to the current TOE. The code review observations, together with the results of the profiling testing, demonstrated that the results of the penetration tests performed on the previous versions of the product are applicable to the current TOE.
67. The Evaluators ran their tests on the configuration defined in Chapter III 'Test Configurations'.
68. The Evaluators completed their period of penetration tests on 2 November 2016.

### *Vulnerability Analysis*

69. 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 SOGIS guidance provided in the [JIL] documentation.

---

***Platform Issues***

70. The TOE is an Embedded Secure Element and no platform issues were identified.

## VI. REFERENCES

[AG]	Administration Guide: Preparative Procedures - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 1.9, 2016-11-14.
[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, 2 <sup>nd</sup> 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]	BSI-DSZ-CC-0915-2016 for BCM_SPS02 Secure Processing System with IC Dedicated Software, Version 1.0 from Broadcom, Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-DSZ-CC-0915-2016, Issue 1.0, 25 February 2016.
[CR_IC_MR]	Assurance Continuity Maintenance Report - BSI-DSZ-CC- 0915-2016-MA-01 - BCM_SPS02 Secure Processing System with Firmware version 002.010 or 002.020, Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-DSZ-CC-0915-2016-MA-01, Issue 1.0, 1 June 2016.

[CWG_MEC HS]	SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.0, May 2016.
[ETR]	SkySIM CX Virgo V3.0 Evaluation Technical Report, UL Transaction Security, UL/SEC/ETR/11477940, Version 1.0, 21 April 2017.
[GP221]	GlobalPlatform Card Specification, GlobalPlatform Inc, Version 2.2.1, January 2011.
[JCAPI304]	Java Card API, Classic Edition, Oracle, Version 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], [JIL_COMP], [JIL_DEL] and [JIL_OPEN]).
[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.
[JIL_DEL]	Security requirements for post-delivery code loading, Joint Interpretation Library, Version 1.0, February 2016.



[JIL_OPEN]	Certification of "open" smart card products, Joint Interpretation Library, Version 1.1 (for trial use), 4 February 2013.
[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]	Java Card Protection Profile, Open Configuration, Oracle Corporation, Version 3.0, May 2012.
[ST]	SkySIM CX Virgo V3.0 Security Target, Giesecke & Devrient GmbH, Issue 4.2, 2016-11-25.
[ST-Lite]	SkySIM CX Virgo V3.0 Security Target Lite, Giesecke & Devrient GmbH, Issue 4.2, 2016-11-25.
[UG]	User Guides: [UG_COMMON] Operational User Guidance Common Document - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 1.8, 2016-11-14.  [UG_AD] Operational User Guidance for the Application Developer - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 2.3, 2016-09-22.  [UG_AP] Operational User Guidance for the Application Provider - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 1.5, 2016-10-04.  [UG_CA] Operational User Guidance for the Controlling Authority - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 1.6, 2016-09-22.  [UG_ISSUER] Operational User Guidance for the Issuer - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 2.0, 2016-11-14.  [UG_PERSONALISER] Operational User Guidance for the Personaliser - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 1.9, 2016-11-14.

	[UG_VA] Operational User Guidance for the Verification Authority - SkySIM CX Virgo V3.0, Giesecke & Devrient GmbH, Issue 1.5, 2016-10-04.
[UKSP00]	UK Scheme Publication No. 00, Abbreviations and References, UK IT Security Evaluation and Certification Scheme, UKSP 00, Issue 1.8, August 2013.
[UKSP01]	UK Scheme Publication No. 01, Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 6.6, August 2014.
[UKSP02]	UK Scheme Publication No. 02, CLEF Requirements (comprising Parts I and II: [UKSP02P1] and [UKSP02P2]).
[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.
[USIM_PP]	(U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations, SFR S.A., Issue 2.0.2, 17 June 2010.

## 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
CRS	Contactless Registry Services
DES	Data Encryption Standard
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eSE	Embedded Secure Element
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
MAC	Message Authentication Code
OS	Operating System
RSA	Rivest Shamir Adleman
SCP	Smart Card Platform
SCP02	Secure Channel Protocol 02
SCP03	Secure Channel Protocol 03
SWP	Single Wire Protocol
TDES	Triple DES
VM	Virtual Machine



---

## VIII. CERTIFICATE

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

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.



Certified Product

*Common Criteria*  
P300



**This is to certify that**

***Giesecke & Devrient GmbH***

**SkySIM CX Virgo  
Version 3.0**

**Running on Broadcom BCM\_SPS02 C0**

*has been evaluated under the terms of the*

***Common Criteria Scheme***  
*and conforms with the requirements for*

**Java Card Protection Profile Open Configuration  
Version 3.0**



**AUTHORISED BY  
DIRECTOR GENERAL  
FOR GOVERNMENT  
AND INDUSTRY CYBER SECURITY**

**THIS PRODUCT WAS EVALUATED BY  
UL Transaction Security**

**DATE AWARDED  
21 April 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](http://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 approved Evaluation Facility of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification 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 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.

*All judgements contained in this certificate, and in the associated Certification Report, are covered by 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 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](http://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 CESG Certification Body's website ([www.ncsc.gov.uk](http://www.ncsc.gov.uk)) provides a reference to the CC Portal ([www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)) for the IT products certified under the UK Scheme. The CC Portal 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 not be trademarks of their respective owners.