122

MAINTENANCE REPORT MR1
(supplementing Certification Report No. CR300)

Sm@rtSIM CX Virgo
Version 5.0

Issue 1.0

August 2017

CESG Certification Body
Industry Enabling Services, NCSC
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

CERTIFICATION STATEMENT (ADDENDUM)

Sponsor	G+D Mobile Security GmbH	Developer	G+D Mobile Security GmbH
Product Name, Version	Sm@rtSIM CX Virgo Version 5.0		
Platform/Integrated Circuit	Broadcom BCM_SPS02 C0		
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		
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[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 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. INTRODUCTION

Overview

1. This Maintenance Report [MR1] states the outcome of the Common Criteria (CC) [CC] Assurance Continuity [AC] process for ***Sm@rtSIM CX Virgo Version 5.0*** - i.e. the 'latest derived version' - as summarised on page 2 of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their requirements.

2. The baseline for this report was the original CC evaluation of ***SkySIM CX Virgo Version 3.0 running on Broadcom BCM_SPS02 C0***, which was certified in April 2017 by the CESG Certification Body to CC EAL4 augmented by ALC_DVS.2 and AVA_VAN.5 - i.e. the 'original certified version' or 'Certified TOE'.

3. The CC Recognition Arrangement (CCRA) [CCRA] requires the Security Target (ST) to be included with the Certification Report. However Appendix I.13 of [CCRA] allows the ST to be sanitised by removing or paraphrasing proprietary technical information; the resulting document is named "ST-lite". Hence for the Target of Evaluation (TOE):

   a) for the original certified version: its ST was [ST] and its ST-lite was [ST_LITE];

   b) for the latest derived version: its ST is [ST1] and its ST-lite is [ST1_LITE].

4. Prospective consumers should read the following documents for the TOE, which are available on the CC website (www.commoncriteriaportal.org) and the NCSC website (www.ncsc.gov.uk):

   - for the original certified version: its [ST_LITE], its Certification Report [CR] and its related Certificate;
   - for the latest derived version: its [ST1_LITE], its Maintenance Report [MR1] (i.e. this document) and its maintenance addendum on the above websites.

5. The Developer of the TOE (i.e. the original certified version and the latest derived version) is G+D Mobile Security GmbH.

Maintained Version(s)

6. The 'original certified version' of the TOE was:

   - SkySIM CX Virgo V3.0, running on Broadcom BCM_SPS02 C0.

7. The 'latest derived version' of the TOE for which assurance is maintained is:

   - Sm@rtSIM CX Virgo Version 5.0, running on Broadcom BCM_SPS02 C0.

8. The maintenance of the latest derived version is described in this report [MR1], which provides a summary of the incremental changes from the original certified version [CR].

Assurance Continuity Process

9. The CCRA [CCRA] is a basis for the mutual international recognition of the results of CC evaluations and certifications. The CC Assurance Continuity process is defined in [AC], and UK specific aspects are defined in UK Scheme Publication 01 [UKSP01] and 03 [UKSP03P1, UKSP03P2]. That process is based on an Impact Analysis Report (IAR) by the Developer. The IAR is intended to describe all changes made to the product, including changes to previously-evaluated evidence, and to assess the security impact of each change.

10. For the latest derived version of the TOE, the Developer followed the above process and the following activities were performed:

a) the Developer made two changes to the software to improve security, as described in the IAR;

b) the Developer made no other changes to the TOE or its development environment, hence no additional security testing was required;

c) the Developer requested CC assurance continuity for the changed environment of the Certified TOE and the application for maintenance was granted by the CESG Certification Body within the two-year guideline stated in [AC].

11. The Developer produced the IAR [IAR1]. The CESG Certification Body examined [IAR1] and the supporting evidence, then produced this report [MR1] and the maintenance addendum on the CC website and the CESG website.

General Points

12. Assurance Continuity addresses the security functionality claimed, with reference to the assumed environment specified, in the ST/ST-lite. For the latest derived version, its scope, configuration and platform environment are summarised in Chapter II of this report [MR1], in conjunction with the original Certification Report [CR]. Prospective consumers are advised to check that this matches their requirements.

II. ASSURANCE MAINTENANCE

Analysis of Changes

13. [IAR1] is the IAR from the certified version of the TOE to the latest derived version of the TOE, and provides the Assurance Continuity rationale for the latest derived version on the stated platform. [IAR1] conforms to the requirements of [AC] and the UK specific aspects in [UKSP01], [UKSP03P1] and [UKSP03P2].

14. No *Major* changes that could cause a security impact on the TOE were made between the certified version and the latest derived version. As noted in [IAR1] Section 3.1, all changes were *Minor* and did not impact the TOE's security functionality.

15. The changes and their impact on the evaluation deliverables are stated in [IAR1] Chapters 3 - 5, which show that for all changes:

a) the impact of each change is determined to be *Minor*;

b) the effect on the previously-evaluated evidence is determined to be *Minor*;

c) the action required for resolution is determined to be *None*, as the previously-evaluated evidence has already been updated, and no further security tests are required.

16. The CESG Certification Body's review of [IAR1] is documented in [REVIEW1] and concurs with the Sponsor's overall conclusion. The changes to the previously-evaluated evidence are summarised in Paragraph 17 of this report.

Changes to Developer Evidence

17. [IAR1] Chapter 4 states that the previously-evaluated evidence that was updated for the latest derived version of the TOE was as follows:

- SkySIM CX Virgo V3.0 Security Target, Version 4.2, 2016-11-25
- Operational User Guidance SkySIM CX Virgo V3.0, Version 1.8, 2016-11-14
- Preparative Procedures SkySIM CX Virgo V3.0, Version 1.9. 2016-09-22
- Configuration List SkySIM CX Virgo V3.0, Version 0.2, 2016-12-02
- TDS_SkySIM_CX_Virgo_v0.19.5.rar
- Test Logs, Version 0.9.15, 2016-11-15All updates in the above documents were classified as *Minor*.

18. No changes were required to the TOE Security Guidance and Java Card Open Platform documentation detailed in [CR].

TOE Identification

19. The latest derived version is uniquely identified in Paragraph 7 of this report.

TOE Scope and TOE Configuration

20. The TOE scope is defined in Section 1.4 of [ST1_LITE].

21. The TOE is the whole product. There is only one possible configuration. Hence the TOE configuration is the product configuration.

TOE Documentation

22. With respect to the Installation, Configuration and Guidance documents listed in the Certification Report for the original certified version of the TOE [CR], there were no changes for the latest derived version of the TOE.

TOE Environment

23. The TOE environment is defined in [ST1_LITE] Sections 7.1 and 8.2

III. TOE TESTING

Vulnerability Analysis

24. In summary, there was no requirement to assess whether any vulnerability had been introduced into the TOE between its original certified version and its latest derived version, as there had been no changes to the TOE or its related development procedures. Therefore there were no new vulnerabilities impacting the TOE and its subsystems.

25. During the evaluation of the original version of the TOE [ETR], the evaluators' vulnerability analysis was based on the JIL *"Attack Methods for Smartcard and Similar Devices"* [JIL_AM] and a search for other public vulnerabilities. No vulnerabilities were found during the original evaluation.

26. A search of a sample of public websites on 7th May confirmed that there were no publicly-known vulnerabilities in the latest derived version of the TOE.

Testing

27. For the latest derived version of the TOE, the Developer did not need to perform any re-testing. The testing performed by the *UL Transaction Security* CLEF for the Certified TOE is described in [CR]. The *UL Transaction Security* CLEF was not required to perform any further tests on the latest maintained version of the TOE.

28. The Developer's tests are comprehensively listed in Chapter 4 of the Configuration List [CL1] for the latest derived version of the TOE and are identical to those in [CL].

29. The Developer holds a copy of the original evaluation's Evaluation Technical Report [ETR]. The Developer does not hold the Evaluators' test scripts and does not update them.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

30. The analysis in [IAR1] shows that no change with a security impact of *Major* has been made to the TOE between the certified version of the TOE and the latest derived version of the TOE.

31. All changes have been categorised as having a security impact of ***Minor*** and hence CC EAL4 augmented by ALC_DVS.2 and AVA_VAN.5 assurance has been maintained.

Conclusions

32. The CESG Certification Body accepts the analysis in [IAR1], which assessed each change as having a security impact of ***Minor***, and concludes that the overall impact of all changes is ***Minor***.

33. The CESG Certification Body has therefore determined that CC EAL4 augmented by ALC_DVS.2 and AVA_VAN.5, as outlined in the Certification Report [CR], has been maintained for the latest derived version of the TOE. These conclusions are summarised in the 'Certification Statement (Addendum)' on Page 2 of this report.

34. Prospective consumers of the latest derived version of the TOE should understand the scope of the maintenance by reading this report in conjunction with [ST1_LITE]. The TOE should be used in accordance with the environmental assumptions specified in [ST1_LITE]. Prospective consumers should check that the Security Functional Requirements (SFRs) and the certified configuration (as maintained for the latest derived version of the TOE) match their requirements, and should give due consideration to the recommendations and caveats of this report.

35. The TOE should be used in accordance with the supporting guidance in the certified configuration, maintained for the latest derived version of the TOE. Recommendations on secure receipt, installation, configuration and operation of the TOE are in the Certification Report [CR].

Disclaimers

36. The Assurance Continuity process is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered afterwards. This report reflects the CESG Certification Body's views on the date of this report.

37. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the vendor to see if any patches exist for the product and whether those patches have further assurance.

38. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. 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.

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

V. REFERENCES

Common Criteria Documents:

[AC] Assurance Continuity: CCRA Requirements,
Common Criteria Development Board,
2012-06-01, Version 2.1, June 2012.

[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-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
2nd July 2014.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8th January 2010 (effective April 2010).

UK IT Security Evaluation and Certification Scheme Documents:

[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.

[UKSP03P1] Sponsor's Guide - General Introduction,
UK IT Security Evaluation and Certification Scheme,
UKSP 03 Part I, Issue 3.1, August 2013.

[UKSP03P2] Sponsor's Guide - Assurance Continuity,
UK IT Security Evaluation and Certification Scheme,
UKSP 03 Part II, Issue 1.3, August 2014.

Original Certified Version:

[CR] Common Criteria Certification Report No. CRP300: Version 1.0, CESG Certification Body, Issue 1.0, April 2017.

[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 and 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.

[ETR] SkySIM CX Virgo V3.0 Evaluation Technical Report, UL Transaction Security, UL/SEC/ETR/11477940, Version 1.0, 21 April 2017.

[JIL_AM] Attack Methods for Smartcards and Similar Devices, Joint Interpretation Library, Version 2.3, July 2012.

[ST] Security Target SkySIM CX Virgo Version 3.0, Giesecke & Devrient GmbH, V4.2 25 November 2016.

[ST_LITE] Security Target Lite SkySIM CX Virgo Version 3.0, Giesecke & Devrient GmbH, V4.2 25 November 2016.

Latest Derived Version:

[CL1] Configuration List SkySIM CX Virgo V3.0, Version 0.2, 2016-12-02.

[CR_IC_MR] Assurance Continuity Maintenance Report BSI-DSZ-CC-0915-2016-MA-03, BCM_SPS02, Secure Processing System with Firmware version 002.030 from NXP, 02.12.2016.

[IAR1] Impact Analysis Report Sm@rtSIM CX Virgo Version 5.0, Giesecke+Devrient Mobile Security GmbH, Version 1.2/18.07.2017

[JIL_MSSR] Minimum Site Security Requirements (MSSR), Joint Interpretation Library, Version 1.1 (for trial use), July 2013.

[MR1] Common Criteria Maintenance Report MR1 *(i.e. this document).*

[REVIEW1] CESG Certification Body Review Form, T024 Virgo 5.0 IAR CB review 25 July 2017

[ST1] Security Target Sm@rtSIM CX Virgo Version 5.0, Giesecke+Devrient Mobile Security GmbH, v4.4 18 July 2017

[ST1_LITE] Security Target Lite Sm@rtSIM CX Virgo Version 5.0,
Giesecke+Devrient Mobile Security GmbH,
v4.4 18 July 2017

VI. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard Common Criteria abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]); and UK Scheme abbreviations and acronyms (e.g. CESG, CLEF) covered in [UKSP00].

MSSR	Minimum Site Security Requirements