Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0976-V3-MA-01

STARCOS 3.7 COS GKV C2

from

Giesecke+Devrient Mobile Security GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developer's Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0976-V3-2019.

The certified product itself did not change. The changes are related to an update of life cycle security aspects, concerning the integration of additional already certified production sites into the scope of the certificate and the renewal of site certificates for development and production sites.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0976-V3-2019 dated 21 November 2019 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0976-V3-2019.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 only

Bonn, 15 June 2021

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the STARCOS 3.7 COS GKV C2, Giesecke+Devrient Mobile Security GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The certified product STARCOS 3.7 COS GKV C2 itself did not change.

The changes are related to an update of life cycle security aspects, concerning the integration of additional already certified production sites into the scope of the certificate and the renewal of site certificates for development and production sites. The ALC re-evaluation was performed by the ITSEF SRC Security Research & Consulting GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [6]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

The list of the development and production sites in Annex B of Certification Report BSI-DSZ-CC-0976-V3-2019 including their related site certificates is replaced as follows:

a) Giesecke+Devrient Mobile Security GmbH Development Center Germany (DCG) for Development and Testing. Refer to the Certification Report BSI-DSZ-CC-S-0132-2019 ([7]).

b) Giesecke+Devrient Mobile Security Iberica S.A.U. Development Center Spain (DCS) for Development. Refer to the Certification Report CCN-CC-8/2021 ([8]).

c) NedCard (Shanghai) Microelectronics Co. Ltd. of NedCard BV for Module Production. Refer to the Certification Report BSI-DSZ-CC-S-0144-2020 ([9]).

d) NedCard B.V. Wijchen for Module Production. Refer to the Certification Report BSI-DSZ-CC-S-0128-2019 ([10]).

e) Shanghai INESA Intelligent Electronics Co. Ltd. for Module Production. Refer to the Certification Report NSCIB-SS-210064-CR ([11]).

f) Giesecke & Devrient Iberica S.A. for Production (in particular inlay embedding) and Initialisation. Refer to the Certification Report CCN-CC-41/2020 ([12]).

g) Giesecke+Devrient (China) Technologies Co. Ltd. Huangshi Branch for Production (in particular inlay embedding) and Initialisation. Refer to the Certification Report CCN-CC-13/2021 ([13]).

h) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V3-2020 ([14]).

Hereby, the renewal of the site certificates in b), c) and f) is covered, and the sites in d), e) and g) are added to the life cycle as further production sites. Please note related to h) that since the TOE's certification BSI-DSZ-CC-0976-V3-2019 the underlying hardware was re-certified under BSI-DSZ-CC-1110-V3-2020. In the course of the present ALC re-evaluation the new certificate ([14]) is taken into account as proof of continuity for development and production security for the hardware part of the TOE.

In their combination, above listed sites fulfil Common Criteria assurance requirements ALC – Life cycle support.

Conclusion

The maintained change is at the level of an update of life cycle security aspects addressing newer site certificates for some development and production sites of the life cycle considered herein as well as the integration of additional production sites into the life cycle. The change has no effect on product assurance.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. The update on the vulnerability assessment of the underlying hardware as outlined in BSI-DSZ-CC-1110-V3-2020 was not considered in this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0976-V3-2019 dated 21 November 2019 is of relevance and has to be considered when using the product.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] Section 9, Para. 4, Clause 2).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

This report is an addendum to the Certification Report [3].

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, Version 2.1, June 2012

[2] Impact Analysis Report, STARCOS 3.7 COS GKV C2, Version 1.1, 04 December 2020, G+D Mobile Security GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-0976-V3-2019 for STARCOS 3.7 COS GKV C2 from Giesecke+Devrient Mobile Security GmbH, 21 November 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[4] Security Target BSI-DSZ-CC-0976-V3-2019, Security Target STARCOS 3.7 COS GKV C2, Version 1.4, 12 September 2019, Giesecke+Devrient Mobile Security GmbH (confidential document)

Security Target Lite BSI-DSZ-CC-0976-V3-2019, Security Target Lite STARCOS 3.7 COS GKV C2, Version 1.4, 12 September 2019, Giesecke+Devrient Mobile Security GmbH (sanitised public document)

[5] Configuration List STARCOS 3.7 COS GKV C2 for BSI-DSZ-CC-0976-V3-MA-01, Version 1.0, 28 April 2021, Giesecke+Devrient Mobile Security GmbH (confidential document)

[6] Evaluation Technical Report for STARCOS 3.7 COS GKV C2, BSI-DSZ-CC-0976-V3-MA-01, Version 2.9, 26 May 2021, SRC Security Research & Consulting GmbH (confidential document)

[7] Certification Report for Giesecke+Devrient Mobile Security GmbH Development Center Germany (DCG), BSI-DSZ-CC-S-0132-2019, 4 October 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[8] Certification Report CCN-CC/2020-47/INF-3465 for Giesecke+Devrient Development Center Spain (DCS), related to CCN-CC-8/2021, 17 May 2021 (Certificate Date), National Cryptologic Centre (CCN)

[9] Certification Report for NedCard (Shanghai) Microelectronics Co. Ltd. of NedCard BV, BSI-DSZ-CC-S-0144-2020, 08 May 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[10] Certification Report for NedCard Wijchen of NedCard BV, BSI-DSZ-CC-S-0128-2019, 16 December 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[11] Certification Report for INESA Shanghai, INESA Intelligent Electronics Co. Ltd., NSCIB-SS-210064-CR, Revision 1, related to NSCIB-SS-210064, 03 September 2019, Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

[12] Certification Report CCN-CC/2019-49/INF-3362 for Giesecke & Devrient Iberica S.A., related to CCN-CC-41/2020, 17 May 2020 (Certificate Date), National Cryptologic Centre (CCN)

[13] Certification Report CCN-CC/2020-35/INF-3504 for Giesecke & Devrient (China) Technologies Co. Ltd. Huangshi Branch, related to CCN-CC-13/2021, 21 May 2021 (Certificate Date), National Cryptologic Centre (CCN)

[14] Certification Report BSI-DSZ-CC-1110-V3-2020 for Infineon Security Controller IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 13 May 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)