Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0976-V4-2021-MA-02

STARCOS 3.7 COS HBA-SMC

from

Giesecke+Devrient ePayments GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] 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-V4-2021 and BSI-DSZ-CC-0976-V4-2021-MA-01.

The certified product itself did not change. The changes are on the one hand related to an update of life cycle security aspects, precisely concerning the renewal of (site) certificates for development and production sites. On the other hand, further changes affect the update of the Security Target [4] and the TOE user guidance documentation [6] regards the TOE’s random number generation functionality.

Considering the nature of the changes leads to the conclusion that these are 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-V4-2021 and Maintenance Report BSI-DSZ-CC-0976-V4-2021-MA-01 dated 18 June 2021 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-V4-2021 and Maintenance Report BSI-DSZ-CC-0976-V4-2021-MA-01.

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

Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bonn, 16 June 2025

The Federal Office for Information Security

Assessment

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [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 HBA-SMC, Giesecke+Devrient ePayments GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [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 HBA-SMC itself did not change.

On the one hand, the changes performed in the present maintenance process are related to an update of life cycle security aspects, more precisely concerning the renewal of (site) certificates for development and production sites. The ALC re-evaluation was supported by the ITSEF SRC Security Research & Consulting GmbH.

The list of the development and production sites in Annex B of the Certification Report BSI-DSZ-CC-0976-V4-2021 and in the Maintenance Report BSI-DSZ-CC-0976-V4-2021-MA-01 including their related site certificates is replaced as follows:

a) Giesecke+Devrient Development Center Germany (DCG) for Development and Testing. Refer to the Certification Report BSI-DSZ-CC-S-0260-2023 [7].

b) Giesecke+Devrient Development Center Spain (DCS) for Development. Refer to the Certification Report CCN-CC/2022-53/INF-4095 and maintenance report CCN-CC/2023-21/INF-4149 [8].

c) Linxens Singapore Changi Site for Module Production. Refer to the Certification Report CCN-CC/2023-01/INF-4274 [9].

d) Linxens Tianjin Site for Module Production. Refer to the Certification Report CCN-CC/2023-35/INF-4423 [10].

e) INESA Shanghai, INESA Intelligent Electronics Co. Ltd. for Module Production. Refer to the Certification Report NSCIB-SS-2300084-01 [11].

f) Giesecke+Devrient ePayments Iberia S.A. (GDIMS) for Production (in particular Inlay Embedding) and Initialisation. Refer to the Certification Report CCN-CC/2024-08/INF-4392 [12].

g) Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch (GDCHINA HS) for Production (in particular Inlay Embedding) and Initialisation. Refer to the Certification Report CCN-CC/2022-46/INF-4163 [13].

h) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V7-2024 [14].

Hereby, the renewal of the site certificates for the development and production sites is covered in a) to g). Please note related to h) that since the TOE's certification BSI-DSZ-CC-0976-V4-2021 the underlying hardware was re-certified under BSI-DSZ-CC-1110-V7-2024. 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 as claimed in the Security Target [4].

Furthermore, the Security Target [4] is updated regards the TOE's random number generation functionality: The SFR FCS_RNG.1 is corrected for being of type DRG.3, and the SFR FCS_RNG.1/PACE is adapted for its reseeding aspect and supplemented by an application note regards the enhanced forward secrecy aspect (refer to the Security Target [4], chapter 6.1.7 and 8.4). The latter is reflected accordingly in an update of the TOE user guidance documentation with a corresponding security requirement for secure use of the TOE's random number generation functionality in case of contactless mode (refer to [6], chapter 5.1.2.6). This change as well was analysed by the ITSEF SRC Security Research & Consulting GmbH.

Conclusion

The maintained changes are on the one hand at the level of an update of life cycle security aspects addressing the renewal of (site) certificates for development and production sites relevant for the life cycle considered herein. These changes have no effect on product assurance.

On the other hand, the further maintained changes are at the level of an update of the Security Target [4] and the TOE user guidance documentation [6]. As well, these changes have no effect on product assurance, but the updated guidance documentation has to be followed (refer to [6], chapter 5.1.2.6).

Considering the nature of the changes performed in the present maintenance process leads to the conclusion that these are 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 of the vulnerability assessment of the underlying hardware as provided in BSI-DSZ-CC-1110-V7-2024 was not considered in this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0976-V4-2021 and the Maintenance Report BSI-DSZ-CC-0976-V4-2021-MA-01 dated 18 June 2021 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 [4] not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The foundation for usage of the certificate updated by this maintenance process is: Regards the TOE user guidance documentation, the updated document version [6] has to be applied, in particular chapter 5.1.2.6 for secure use of the TOE’s random number generation functionality in contactless mode has to be taken into account.

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.

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3], chapter 9.2. However, for consistency and due to the update of the Security Target [4], chapter 6.1.7 concerning the TOE’s random number generation functionality, the entry DRG.4 in row no 26 of Table 5 in [3], Annex C with the overview of the TOE’s cryptographic functionality has to be replaced by DRG.3.

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).

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 3.1, 29 February 2024

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, Version 1.2, March 2024

[2] Impact Analysis Report, STARCOS 3.7 COS HBA-SMC, Version 1.1, 8 May 2025, Giesecke+Devrient ePayments GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-0976-V4-2021 for STARCOS 3.7 COS HBA-SMC from Giesecke+Devrient ePayments GmbH, Version 1.0, 18 June 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[4] Security Target BSI-DSZ-CC-0976-V4-2021-MA-02, Security Target STARCOS 3.7 COS HBA-SMC, Version 2.1, 19 May 2025, Giesecke+Devrient ePayments GmbH (confidential document)

Security Target Lite BSI-DSZ-CC-0976-V4-2021-MA-02, Security Target Lite STARCOS 3.7 COS HBA-SMC, Version 2.1, 19 May 2025, Giesecke+Devrient ePayments GmbH (sanitised public document)

[5] Configuration List STARCOS 3.7 COS HBA-SMC for BSI-DSZ-CC-0976-V4-2021-MA-02, Version 1.0, 19 May 2025, Giesecke+Devrient ePayments GmbH (confidential document)

[6] Guidance Documentation for the Usage Phase STARCOS 3.7 COS HBA-SMC, Version 1.9, 19 May 2025, Giesecke+Devrient ePayments GmbH

[7] Certification Report for Giesecke+Devrient Development Center Germany (DCG) of Giesecke+Devrient ePayments GmbH, BSI-DSZ-CC-S-0260-2023, 20 December 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[8] Certification Report CCN-CC/2022-53/INF-4095 and maintenance report CCN-CC/2023-21/INF-4149 for Giesecke+Devrient Development Center Spain (DCS), related to CCN-CC-15/2023, 17 May 2023 (Certificate´date), National Cryptologic Centre (CCN)

[9] Certification Report CCN-CC/2023-01/INF-4274 for Linxens Singapore Changi Site, related to CCN-CC-2/2024, 29 February 2024 (Certificate date), National Cryptologic Centre (CCN)

[10] Certification Report CCN-CC/2023-35/INF-4423 for Linxens Tianjin Site, related to CCN-CC-24/2024, 21 October 2024 (Certificate date), National Cryptologic Centre (CCN)

[11] Certification Report NSCIB-SS-2300084-01 for INESA Shanghai, INESA Intelligent Electronics Co. Ltd., related to NSCIB-SS-2300084-01, 14 August 2023, Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

[12] Certification Report CCN-CC/2024-08/INF-4392 for Giesecke+Devrient ePayments Iberia S.A. (GDIMS), related to CCN-CC-18/2024, 6 September 2024 (Certificate date), National Cryptologic Centre (CCN)

[13] Certification Report CCN-CC/2022-46/INF-4163 for Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch (GDCHINA HS), related to CCN-CC-31/2023, 18 August 2023 (Certificate date), National Cryptologic Centre (CCN)

[14] Certification Report BSI-DSZ-CC-1110-V7-2024 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 30 September 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Note: End of report