Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1077-V2-2024-MA-01

STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2

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-1077-V2-2024.

The certified product itself did not change. The changes are related to an update of the Security Target [4] and the TOE user guidance documentation [7] regarding 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-1077-V2-2024 dated 12 June 2024 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-1077-V2-2024.

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

Bonn, 24 June 2025

The Federal Office for Information Security

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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 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 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, 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 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2 itself did not change.

The changes performed in the present maintenance process are related to an update of the Security Target [4] regarding the TOE's random number generation functionality: The SFR FCS_RND.1/EAC2PP (and correspondingly FCS_RND.1/EAC1PP) is adapted for its reseeding aspect and supplemented by an application note regarding the enhanced forward secrecy aspect (refer to the Security Target [4], chapter 6.1.1). The latter is reflected accordingly in an update of the TOE user guidance documentation [7] with a corresponding security requirement for secure use of the TOE's random number generation functionality in case of contactless mode (refer to [7], chapter 5.1). The changes were analysed by the ITSEF SRC Security Research & Consulting GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [6].

Conclusion

The maintained changes are at the level of an update of the Security Target [4] and the TOE user guidance documentation [7]. These changes have no effect on product assurance, but the updated guidance documentation has to be followed (refer to [7], chapter 5.1).

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-1077-V2-2024 dated 12 June 2024 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: Regarding the TOE user guidance documentation, the updated document version [7] has to be applied, in particular chapter 5.1 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.

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 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, Version 0.2, 31 March 2025, Giesecke+Devrient ePayments GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-1077-V2-2024 for STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2 from Giesecke+Devrient ePayments GmbH, Version 1.0, 12 June 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[4] Security Target BSI-DSZ-CC-1077-V2-2024-MA-01, Security Target STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, Version 1.8, 27 March 2025, Giesecke+Devrient ePayments GmbH (confidential document)

Security Target Lite BSI-DSZ-CC-1077-V2-2024-MA-01, Security Target Lite STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, Version 1.8, 2 June 2025, Giesecke+Devrient ePayments GmbH (sanitised public document)

[5] Configuration List STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2 for BSI-DSZ-CC-1077-V2-2024-MA-01, Version 1.0, 2 June 2025, Giesecke+Devrient ePayments GmbH (confidential document)

[6] Evaluation Technical Report for STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, BSI-DSZ-CC-1077-V2-2024-MA-01, Version 1.1, 2 June 2025, SRC Security Research & Consulting GmbH (confidential document)

[7] Guidance Documentation for the Usage Phase STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, Version 1.7, 27 March 2025, Giesecke+Devrient ePayments GmbH

Note: End of report