Federal Office
for Information Security

Assurance Continuity Reassessment Report

BSI-DSZ-CC-1077-V2-2024-RA-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 certified under the certification procedure BSI-DSZ-CC-1077-V2-2024 amended by the Assurance Maintenance procedure BSI-DSZ-CC-1077-V2-2024-MA-01 [6] has undergone a reassessment of the vulnerability analysis according to the current state of the art attack methods according to the procedures on Assurance Continuity [5], based on the Security Target [7].

This reassessment confirms resistance of the product against attacks on the level of AVA_VAN.5 as stated in the product certificate.

More details are outlined on the following pages of this report.

This report is an addendum to the Certification Report BSI-DSZ-CC-1077-V2-2024 and BSI-DSZ-CC-1077-V2-2024-MA-01.

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

Bonn, 10 December 2025

The Federal Office for Information Security

Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Assessment

The reassessment was performed based on CC [1], CEM [2], according to the procedures on Assurance Continuity [5] and relevant AIS [4] and according to the BSI Certification Procedures [3] by the IT Security Evaluation Facility (ITSEF) SRC Security Research & Consulting GmbH, approved by BSI.

The following guidance specific for the technology has been applied as a refinement of CC and CEM:

- Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to [10]) and the document ETR for composite evaluation from the IC's evaluation ([12]) have been applied in the TOE evaluation.
- Guidance for Smartcard Evaluation (AIS 37, see [4]).
- Attack Methods for Smart Cards and similar devices, under consideration of the current versions of the JIWG/JHAS documents 'Attack Methods for Smartcards and Similar Devices', Version 2.5 and 'Application of Attack Potential to Smartcards and Similar Devices', Version 3.2.1 (AIS 26, see [4]).
- Application of Attack Potential to Smartcards (AIS 26, see [4]).
- Application of CC to Integrated Circuits (AIS 25, see [4]).
- Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).
- Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4]).
- Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).
- Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

The results of the reassessment of the product STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2 are documented in an updated version of the ETR [8].

Please note that the product STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2 is set up on the Infineon Security Controller IFX_CCI_000005h that was originally certified under the Certification ID BSI-DSZ-CC-1110-V6-2023 (refer to BSI-DSZ-CC-1077-V2-2024 [6]). In the meantime, the IC platform was re-certified under the Certification ID BSI-DSZ-CC-1110-V8-2025 (refer to [10]). For the present reassessment of the TOE, the corresponding updated ETR for composite evaluation [12] and IC user guidance documentation as referenced in [10] were taken into account.

Regarding cryptographic security functionality:

Cryptographic security functionality as well is considered within the scope of a reassessment.

No changes applied regarding cryptographic security functionality. The previous certification report [6] still applies in that regard.

Regarding assurance class life cycle (ALC):

The assurance class ALC as well is considered within the scope of a reassessment.

The following ALC aspects with regard to the conducted vulnerability assessment changed, compared to the previous certification and the subsequent maintenance procedure:

- Renewal of site certificates

Whereas the site certificate for the Giesecke+Devrient ePayments Development Centre Germany (DCG) [13] is unchanged, the site certificates for the following sites were updated:

- Linxens (Thailand) Co Ltd. [14]
- Bundesdruckerei GmbH [15]

Please refer to [13], [14] and [15] for details.

For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V8-2025 [10].

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Securtiy Target [7].

The obligations and recommendations as outlined in the certification and maintenance reports [6] are still valid and have to be considered. Refer in particular to the certification report, chapters 10 and 12, and the maintenance report, section “Obligations and notes for the usage of the product”.

The obligations and recommendations as outlined in the guidance documentation referenced in [6] have to be considered by the user of the product.

The assessment on TOE cryptographic security functionality did not change in comparison to the previous certification and maintenance procedure [6].

Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte)
https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[1]
https://www.bsi.bund.de/AIS

[5] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 3.0, March 2023

[1] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document (under consideration of the current versions of the JIWG/JHAS documents ‘Attack Methods for Smartcards and Similar Devices’, Version 2.5 and ‘Application of Attack Potential to Smartcards and Similar Devices’, Version 3.2.1)
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document (but with usage of updated JIL document ‘Composite product evaluation for Smart Cards and similar devices’, version 1.5.1, May 2018)
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.1, June 2023

[6] 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, 12 June 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)

amended by the following Assurance Continuity Maintenance Report:

Assurance Continuity Maintenance Report BSI-DSZ-CC-1077-V2-2024-MA-01 for STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, 24 June 2025, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[7] 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)

[8] Evaluation Technical Report BSI-DSZ-CC-1077-V2-2024-RA-01, Evaluation Report Re-Assessment – Evaluation Technical Report (ETR) – Summary for STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, Version 1.2, 13 October 2025, SRC Security Research & Consulting GmbH (confidential document)

[9] Configuration List BSI-DSZ-CC-1077-V2-2024-RA-01, Configuration List STARCOS 3.7 ID ePA C2, STARCOS 3.7 ID eAT C2, STARCOS 3.7 ID ePass C2, Version 1.2, 21 July 2025, Giesecke+Devrient ePayments GmbH (confidential document)

[10] Certification Report BSI-DSZ-CC-1110-V8-2025 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, 5 August 2025, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[11] Security Target Lite of the underlying hardware platform, Common Criteria Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13, Revision 6.2, 26 June 2025, Infineon Technologies AG, BSI-DSZ-CC-1110-V8-2025 (sanitised public document)

[12] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h, H13 from certification procedure BSI-DSZ-CC-1110-V8-2025, Version 2, 25 July 2025, TÜV Informationstechnik GmbH (confidential document)

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

[14] Site Certification Report BSI-DSZ-CC-S-0281-2024 for Linxens (Thailand) Co Ltd.,13 June 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[15] Site Certification Report BSI-DSZ-CC-S-0273-2024 for Bundesdruckerei GmbH manufacturing site for ePassport, eCover, eID card, RP card, -inlay of Bundesdruckerei GmbH, 19 July 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)

End of report