Federal Office
for Information Security

Assurance Continuity Reassessment Report

BSI-DSZ-CC-1077-2020-RA-01

STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

from

Giesecke+Devrient Mobile Security GmbH

SOGIS
Recognition Agreement

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-1077-2020 [5] has undergone a re-assessment of the vulnerability analysis according to the current state of the art attack methods and based on the Security Target [6].

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-1077-2020.

Common Criteria
Recognition
Arrangement
for components up to
EAL 2 only

Bonn, 9 February 2022

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 reassessment was performed based on CC [1], CEM [2] 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 [9]) and the document ETR for composite evaluation from the IC's evaluation ([11]) have been applied in the TOE evaluation.
- Guidance for Smartcard Evaluation (AIS 37, see [4]).
- Attack Methods for Smartcards and Similar Devices, under consideration of the current versions of the JIWG/JHAS documents 'Attack Methods for Smartcards and Similar Devices', Version 2.4 and 'Application of Attack Potential to Smartcards and Similar Devices', Version 3.1 (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]).

Please note that the product STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 is set up on the Infineon Security Controller IFX_CCI_000005h that was originally certified under the Certification ID BSI-DSZ-CC-1110-V3-2020 (refer to BSI-DSZ-CC-1077-2020, [5]). In the meantime, the IC platform was re-certified under the Certification ID BSI-DSZ-CC-1110-V4-2021 (refer to [9]). For the present reassessment, the corresponding updated ETR for composite evaluation [11] and IC user guidance documentation as referenced in [9] were taken into account.

Concerning the ALC aspect, the renewal of site certificates as relevant for the TOE was considered for the reassessment, refer to [12], [13] and [14]. In addition, a minor adaptation of the TOE's production processes was addressed by the reassessment. A corresponding update of the TOE's configuration list was provided ([8]).

The results of the reassessment of the product STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 are documented in an updated version of the ETR [7].

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Security Target [6].

The obligations and recommendations as outlined in the certification report [5] for BSI-DSZ-CC-1077-2020 are still valid and have to be considered. Refer in particular to [5], chapters 10 and 12.

The obligations and recommendations as outlined in the product's guidance documentation referenced in [5] have to be considered by the user of the product.

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
https://www.commoncriteriaportal.org

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

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
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] Certification Report BSI-DSZ-CC-1077-2020 for STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, 5 August 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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 2.4 and ‘Application of Attack Potential to Smartcards and Similar Devices’, Version 3.1)
- 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 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

[6] Security Target BSI-DSZ-CC-1077-2020, Security Target STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 1.11, 16 July 2020, Giesecke+Devrient Mobile Security GmbH (confidential document)

Security Target Lite BSI-DSZ-CC-1077-2020, Security Target Lite STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 1.11, 16 July 2020, Giesecke+Devrient Mobile Security GmbH (sanitised public document)

[7] Evaluation Technical Report BSI-DSZ-CC-1077-2020-RA-01, Evaluation Report Re-Assessment – Evaluation Technical Report (ETR) – Summary for STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 1.4, 2 February 2022, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration List BSI-DSZ-CC-1077-2020-RA-01, Configuration List STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 0.28, 20 December 2021, Giesecke+Devrient Mobile Security GmbH (confidential document)

[9] Certification Report BSI-DSZ-CC-1110-V4-2021 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, 4 August 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[10] Security Target of the underlying hardware platform, Common Criteria Confidential 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 3.4, 18 May 2021, Infineon Technologies AG, BSI-DSZ-CC-1110-V4-2021 (confidential document)

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 1.9, 18 May 2021, Infineon Technologies AG, BSI-DSZ-CC-1110-V4-2021 (sanitised public document)

[11] 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-V4-2021, Version 1, 1 July 2021, TÜV Informationstechnik GmbH (confidential document)

[12] Site Certification Report BSI-DSZ-CC-S-0185-2021 for Giesecke+Devrient Mobile Security Development Center Germany, 4 October 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] Site Certification Report CCN-CC/2020-47/INF-3465 to CCN-CC-8/2021 for Giesecke+Devrient Mobile Security Iberica S.A.U. - Development Center Spain, 18 March 2021, National Cryptologic Centre (CCN)

[14] Site Certification Report BSI-DSZ-CC-S-0207-2021 for Linxens (Thailand) Co Ltd., 24 November 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)