Federal Office
for Information Security

Assurance Continuity Reassessment Report

BSI-DSZ-CC-1188-2023-RA-01

TCOS ID Version 3.0 Release 1/P71

from

Deutsche Telekom Security GmbH

SOGIS
Recognition Agreement

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-1188-2023 [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-1188-2023.

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

Bonn, 25 October 2024

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], 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 have 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 2.5 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 TCOS ID Version 3.0 Release 1/P71 are documented in an updated version of the ETR [8].

Please note that the product TCOS ID Version 3.0 Release 1/P71 is set up on the NXP Secure Smart Card Controller N7122 that was originally certified under the Certification ID BSI-DSZ-CC-1149-2022 and BSI-DSZ-CC-1149-2022-MA-01 (refer to BSI-DSZ-CC-1188-2023, [6]). In the meantime, the IC platform was re-certified under the Certification ID BSI-DSZ-CC-1149-V3-2023 (refer to [9]). For the present reassessment of the TOE, the corresponding updated ETR for composite evaluation [11] and IC user guidance documentation as referenced in [9] 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 aspect with regard to the conducted vulnerability assessment changed, compared to the previous certification:

- renewal of site certificates and audits

Especially the site certificate for the following site was renewed:

- Bundesdruckerei GmbH [12]

Please refer to [12] for details.

Changes of ALC related aspects concerning the underlying NXP IC platform are covered by [9].

Conclusion

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

The obligations and recommendations as outlined in the certification report [6] are still valid and have to be considered.

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 [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
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)
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, 09 March 2023
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.1, June 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 2.4 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] Certification Report BSI-DSZ-CC-1188-2023 for TCOS ID Version 3.0 Release 1/P71, 18 April 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[7] Security Target BSI-DSZ-CC-1188-2023, Specification of the Security Target TCOS ID Version 3.0 Release 1/P71, Version 3.0.1, 27 March 2023, Deutsche Telekom Security GmbH

[8] Evaluation Technical Report BSI-DSZ-CC-1188-2023-RA-01, Evaluation Report Re-Assessment – Evaluation Technical Report (ETR) – Summary for TCOS ID Version 3.0 Release 1/P71, Version 1.0, 21 October 2024, SRC Security Research & Consulting GmbH (confidential document)

[9] Certification Report BSI-DSZ-CC-1149-V3-2023 for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) from NXP Semiconductors Germany GmbH, 13 December 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[10] Security Target Lite BSI-DSZ-CC-1149-V3-2023, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 1.8, 01 December 2023, NXP Semiconductors Germany GmbH (sanitised public document)

[11] Evaluation Technical Report for Composite Evaluation (ETR COMP), BSI-DSZ-CC-1149-V3-2023, Version 2, 01 December 2023, TÜV Informationstechnik GmbH (confidential document)

[12] Site Certification Report BSI-DSZ-CC-S-0273-2024 for Bundesdruckerei (bdr) manufacturing site, 19 July 2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)