Federal Office
for Information Security

Assurance Continuity Reassessment Report

BSI-DSZ-CC-1078-RA-01

TCOS ID Version 2.0 Release1/P6022y

from

Deutsche Telekom Security GmbH

SOGIS
Recognition Agreement

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-1078-2019 [5] has undergone a reassessment 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-1078-2019.

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

Bonn, 15 June 2021

The Federal Office for Information Security

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

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 [15]) and the document ETR for composite evaluation from the IC's evaluation ([16]) have been applied in the TOE evaluation.
- Guidance for Smartcard Evaluation (AIS 37, see [4]).
- Attack Methods for Smartcards and Similar Devices (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 are documented in an updated version of the ETR [7]. Please note, that the present reassessment does not cover a re-evaluation of any RSA-related functionality that was additionally beyond the TOE scope evaluated in the framework of the base certification BSI-DSZ-CC-1078-2019.

Note: In the meantime, the developer's company name changed from T-Systems International GmbH to Deutsche Telekom Security GmbH.

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Security Target [6]. Hereby, the reassessment only covers the TOE related functionality and in particular does not include any RSA-related functionality.

The obligations and recommendations as outlined in the certification report [5] are still valid and have to be considered.

The obligations and recommendations as outlined in the guidance documentation [8] to [14] 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-1078-2019 for TCOS ID Version 2.0 Release1/P6022y, 30 August 2019, Bundesamt für Sicherheit in der Informationstechnik

[6] Security Target BSI-DSZ-CC-1078-2019, Specification of the Security Target TCOS ID Version 2.0 Release1/P6022y, Version 2.0.1, 26 July 2019, T-Systems International GmbH

[1] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- 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
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluierungsmethodologie für die Vertrauenswürdigkeitsklasse EAL5+
- AIS 36, Version 5, ETR-Zusatz zur Unterstützung von Smartcard Kompositionszertifizierungen (ETR for composition) including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[7] Evaluation Technical Report BSI-DSZ-CC-1078-RA-01, Evaluation Technical Report (ETR) - TCOS ID Version 2.0 Release 1/P60D145, Version 1.1, 7 May 2021, SRC Security Research & Consulting GmbH (confidential document)

[8] TCOS ID Version 2.0 Release 1, Guidance Document - Common Part, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, Version 1.0.1, 29 July 2019, T-Systems International GmbH

[9] TCOS ID Version 2.0 Release 1, Operational Guidance - Residence Permit, Guidance Documentation of TCOS ID Version 2.0 Release 1 with ePassport, eID and eSign Application, Version 1.0.1, 14 May 2019, T-Systems International GmbH

[10] TCOS ID Version 2.0 Release 1, Operational Guidance - Passport, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC protocol, Version 1.0.1, 14 May 2019, T-Systems International GmbH

[11] TCOS ID Version 2.0 Release 1, Operational Guidance – Electronic Document, Guidance Documentation of TCOS ID Version 2.0 Release 1 with ePassport, eID and eSign Application, Version 1.0.1, 14 May 2019, T-Systems International GmbH

[12] TCOS ID Version 2.0 Release 1, Administrator's Guidance - Residence Permit, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, Version 1.0.1, 14 May 2019, T-Systems International GmbH

[13] TCOS ID Version 2.0 Release 1, Administrator's Guidance - Passport, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, Version 1.0.1, 14 May 2019, T-Systems International GmbH

[14] TCOS ID Version 2.0 Release 1, Administrator's Guidance – Electronic Document, Guidance Documentation of TCOS ID Version 2.0 Release 1 with PACE/SAC and EAC/PSA protocol, Version 1.0.1, 14 May 2019, T-Systems International GmbH

[15] Certification Report BSI-DSZ-CC-1059-V3-2019 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH, 29 November 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[16] Evaluation Technical Report for Composite Evaluation (ETR-COMP), BSI-DSZ-CC-1059-V3, Version 2, 20 November 2019, TÜV Informationstechnik GmbH (confidential document)