Federal Office
for Information Security

Assurance Continuity Reassessment Report

BSI-DSZ-CC-1121-2019-RA-01

swissbit TSE Version 1.0.4 / 1.0.3

from

Swissbit AG

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-1121-2019 [6] has undergone a re-assessment 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.2 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-1121-2019.

Common Criteria

Bonn, 12 December 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, approved by BSI.

The results are documented in an updated version of the ETR [8].

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.

No changes applied to the assurance aspect ALC. The previous certification report [6] still applies in that regard.

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.2 as claimed in the Security Target [7].

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

The obligations and recommendations as outlined in the guidance documentation [9] 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
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, 2023-03-09,
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.1, June 2023

[6] Certification Report BSI-DSZ-CC-1121-2019 for Swissbit TSE SMAERS Firmware from Swissbit Germany AG, Bundesamt für Sicherheit in der Informationstechnik, 19. December 2019

[7] Security Target BSI-DSZ-CC-1121-2019, Version 1.8.4, 2019-12-13, “Swissbit TSE SMAERS Firmware”, Swissbit AG

[8] Evaluation Technical Report, Version 2.8, 2024-12-11, “Evaluation Technical Report ETR Part Summary”, SRC Security Research & Consulting GmbH

1 specifically

- AIS 20 Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallsgeneratoren für Evaluationen nach Common Criteria und ITSEC, Version 3, 15.05.2013
- AIS 46 Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik