

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0822-V3-2021-RA-02

SMARTY IQ_LTE, Version 1.1

Hardware Version: DNT8209/3.3

Software Version: 2.0.3036

Operating System Version: DNT8209-21

from

Sagemcom Dr. Neuhaus GmbH



SOGIS
Recognition Agreement
for components up to
EAL 4

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-0822-V3-2021 amended by Assurance Maintenance Procedures [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.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-0822-V3-2021.



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

Bonn, 25 November 2024

The Federal Office for Information Security



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 ITSecurity Evaluation Facility (ITSEF) TÜV Informationstechnik GmbH, approved by BSI.

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

Within the scope of the previous reassessment, the guidance documentation related to the product has been updated (see [9] and [10]), replacing the guidance documentation as listed in [6] (reference [10] and [11] in [6]).

Within the scope of this reassessment, the guidance documentation remains unchanged.

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

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.5 as claimed in the Security Target [7].

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

The obligations and recommendations as outlined in the guidance documentation [9] 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
<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 TOE¹ <https://www.bsi.bund.de/AIS>

¹ specifically

- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ and EAL 6

- [5] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 3.1, 29 February 2024
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.2, March 2024
- [6] Certification Report BSI-DSZ-CC-0822-V3-2021 for SMARTY IQ-LTE, Version 1.1, 30 March 2021, Bundesamt für Sicherheit in der Informationstechnik, amended by the following Assurance Continuity Maintenance Reports:
Assurance Continuity Maintenance Report BSI-DSZ-CC-0822-V3-2021-MA-01 for SMARTY IQ-LTE, Version 1.1, 01 April 2022, Bundesamt für Sicherheit in der Informationstechnik
Assurance Continuity Maintenance Report BSI-DSZ-CC-0822-V3-2021-MA-02 for SMARTY IQ-LTE, Version 1.1, 02 September 2022, Bundesamt für Sicherheit in der Informationstechnik
- [7] Security Target BSI-DSZ-CC-0822-V3-2021-RA-01, Version 1.32, 16 February 2023, SMARTY IQ-SMGW LTE Security Target, Sagemcom Dr. Neuhaus GmbH
- [8] Evaluation Technical Report BSI-DSZ-CC-0822-V3-2021-RA-02, Version 1, 08 November 2024, TÜV Informationstechnik GmbH (confidential document)
- [9] Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, Version 1.29, 16 February 2023, Sagemcom Dr. Neuhaus GmbH
hash256:
'd5eaad5fe0ab6d2d1318149ea92e4d1420ae8d44b10862aa83cfd785a25a0424
- [10] Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, Version 1.27, 15 February 2023, Sagemcom Dr. Neuhaus GmbH
hash256:
18cf12a2614037fc2799010224ffb181240b83caf869dc4eec02a989999a105e
- [11] Sichere Lieferkette, Version 1.3, 13 September 2019, Sagemcom Dr. Neuhaus GmbH
hash256:
3ad99a0fa18b7918821ac70255a031d4b0d88c64ea57cd22402748be8b21b375
- [12] Anlage zum AGD: - Http Gateway Protocol 2.4, Version 2.4.026, 22 January 2019, Sagemcom Dr. Neuhaus GmbH
hash256:
7448a50402a3c47331429e932353575b72fedb2743e928dd2fc8eed1ef8c3049
- [13] Anlage zum AGD: Übersicht der Audit Records, Version 1.37, Sagemcom Dr. Neuhaus GmbH
hash256:
c99697f8e87cc93d3c74607de72b110c8691872b066cd8e5c5c9ec5d052bb439
- [14] Anlage zum AGD: Übersicht der versendeten Events, Version 1.37, Sagemcom Dr. Neuhaus GmbH
hash256:
dc4db45ea26695784682b47edda59edcab5bf506df1718ef63ac53b34f748339