

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0822-V5-2023-RA-01

SMARTY IQ-LTE, Version 1.3

Hardware Version: DNT8209/3.3/A and DNT8209/3.3/B

Software Version: 2.1.5003

Operating System Version: DNT8233-04

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-V5-2023 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-V5-2023.



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

Bonn, 9 October 2025

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 IT Security Evaluation Facility (ITSEF) TÜV Informationstechnik GmbH, 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.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 unchanged guidance documentation [9] to [14] 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
<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>
- [5] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 3.1, 2024-02-29,
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.2, March 2024
- [6] Certification Report BSI-DSZ-CC-0822-V5-2023 for SMARTY IQ-LTE, Version 1.3, Bundesamt für Sicherheit in der Informationstechnik, 10 October 2023
amended by the following Assurance Maintenance Reports:
BSI-DSZ-CC-0822-V5-2023-MA-01
- [7] Security Target BSI-DSZ-CC-0822-V5-2023-MA-01, Version 1.153, 2025-05-15, SMARTY IQ-LTE Security Target, Sagemcom Dr. Neuhaus GmbH
- [8] Evaluation Technical Report BSI-DSZ-CC-0822-V5-2023-RA-01, Version 1, 2025-09-19, TÜV Informationstechnik GmbH (confidential document)
- [9] Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, Version 1.107, 2023-01-24, Sagemcom Dr. Neuhaus GmbH
- [10] Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, Version 1.150, 2023-05-26, Sagemcom Dr. Neuhaus GmbH
- [11] Sichere Lieferkette, Version 1.200, 2025-05-16, Sagemcom Dr. Neuhaus GmbH
- [12] Anlage zum AGD: SMGW - Http Gateway Protocol 2.5, Version 2.5.150, 2023-05-19, Sagemcom Dr. Neuhaus GmbH
- [13] Anlage zum AGD: Übersicht der Audit Records, Version 1.108, Sagemcom Dr. Neuhaus GmbH
- [14] Anlage zum AGD: Übersicht der versendeten Events, Version 1.108, Sagemcom Dr. Neuhaus GmbH

¹ specifically

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