



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0822-V3-2021-MA-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 was assessed according to the *Assurance Continuity: CCRA Requirements*, version 2.1, June 2012 and the developer's Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0822-V3-2021 updated by BSI-DSZ-CC-0822-V3-2021-MA-01.

The change to the certified product is at the level of the hardware implementation representation and the guidance documentation. The identification of the maintained product remains the same.

Considering the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0822-V3-2021 dated 30 March 2021 is of relevance and has to be considered when using the product. Details can be found on the following pages.

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



Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bonn, 2 September 2022

The Federal Office for Information Security

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the SMARTY IQ-LTE, Version 1.1, Sagemcom Dr. Neuhaus GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The SMARTY IQ-LTE, Version 1.1, was changed due to allow the usage of an alternative similarly constructed variant of two electronic components. The TOE version number remains the same as the alternative components have the same behaviour as the original ones.

Additionally the guidance documentation [6] and [7] was updated to change an organisational step during the final personalisation process performed by the gateway administrator.

The Security Target [4] and the configuration list [5] were updated accordingly.

Conclusion

The maintained change is at the level of the hardware implementation representation and the guidance documentation. The change has no effect on product assurance.

Considering the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0822-V3-2021 dated 30 March 2021 is of relevance and has to be considered when using the product.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG¹ Section 9, Para. 4, Clause 2).

This report is an addendum to the Certification Report [3].

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

- [1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012
- [2] Impact Analysis Report (IAR), Version 0.4, 2022-09-29, Sagemcom Dr. Neuhaus GmbH (confidential document)
- [3] Certification Report BSI-DSZ-CC-0822-V3-2021 for SMARTY IQ-LTE, Version 1.1, 30 March 2021, Bundesamt für Sicherheit in der Informationstechnik
- [4] Security Target BSI-DSZ-CC-0822-V3-2021-MA-02, Version 1.31, 2022-09-28, SMARTY IQ-SMGW LTE Security Target, Sagemcom Dr. Neuhaus GmbH
- [5] Configuration lists changed for this maintenance procedure:
8209SE030 SMGw Basis LTE_1_3_20220727.xls, Sagemcom Dr. Neuhaus GmbH (confidential document)
filelist3036_solution_documentation__20220928.txt, Sagemcom Dr. Neuhaus GmbH (confidential document)
- [6] Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, Version 1.28, 2022-09-28, Sagemcom Dr. Neuhaus GmbH
SHA256-Hashsum:
ea9ad5588bb0058c848e7ef7476240fb87cc47022787e79451026591cbc676b2
- [7] Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, Version 1.26, 2022-09-28, Sagemcom Dr. Neuhaus GmbH
SHA256-Hashsum:
884e60f5b944f05a4332e3ca1d75f3a7cd4102f3c65c255b539c96b5f7202846