

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0831-V4-2021-RA-02

SMGW, Version 1.2
SMGW, Version 1.2.1
SMGW, Version 1.2.2

from

Power Plus Communications AG



SOGIS
Recognition Agreement
for components up to
EAL 4

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-0831-V4-2021 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-0831-V4-2021.



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

Bonn, 4 September 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].

Within the scope of this reassessment the guidance documentation related to the product has not been updated.

Regarding cryptographic security functionality:

Cryptographic security functionality as well is considered within the scope of a reassessment.

No changes were applied regarding cryptographic security functionality. The previous certification and maintenance reports [6] still apply 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 were applied to the assurance aspect ALC. The previous certification and maintenance reports [6] still apply 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 [11] 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 3.0, 2023-03-09,
Common Criteria document "Assurance Continuity: SOG-IS Requirements", version 1.1, June 2023
- [6] Certification Report BSI-DSZ-CC-0831-V4-2021 for SMGW Version 1.2, Bundesamt für Sicherheit in der Informationstechnik, 05.09.2021
amended by the following Assurance Maintenance Reports:
BSI-DSZ-CC-0831-V4-2021-MA-01
BSI-DSZ-CC-0831-V4-2021-MA-02
BSI-DSZ-CC-0831-V4-2021-MA-03
BSI-DSZ-CC-0831-V4-2021-MA-04
- [7] Security Target SMGW Version 1.2.2, Version 5.1.1, 2023-08-31, Power Plus Communications AG
- [8] Evaluation Technical Report, Version 1, 2025-08-15, TÜV Informationstechnik GmbH (confidential document)
- [9] Handbuch für Hersteller und Betreiber von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway, Version 4.6.1, 2023-08-31, Power Plus Communications AG
SHA-256 hash value:
fc9d4430172fcf671a497fd984bfa526938001a259903cfe0657d4b3801789d5
- [10] Handbuch für Verbraucher, Smart Meter Gateway, Version 4.8, 2022-01-02, Power Plus Communications AG
SHA-256 hash value:
F89231C01A7BB65F9B4BD216E8ED33AC13DBDA95AEBFFD2B4F08CBFD62873CFD

¹ specifically

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

- [11] Handbuch für Service-Techniker, Smart Meter Gateway, Version 5.1, 2022-01-02,
Power Plus Communications AG
SHA-256 hash value:
838C436B1CB26919574AEF68A67D2BEA3A312CD30DB3689871FF8D7E87F2
8B2C