Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0831-V5-2022-MA-02

SMGW, Version 2.0

from

Power Plus Communications AG

SOGIS
Recognition Agreement
for components up to
EAL 4

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] 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-0831-V5-2022 updated by BSI-DSZ-CC-0831-V5-2022-MA-01 and a re-assessment [5] dated 18 December 2024.

The certified product itself did not change. The changes are related to a change concerning the certified scope of the delivery procedures.

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-0831-V5-2022 dated 20 December 2022 updated by a re-assessment [5] on 18 December 2024 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-0831-V5-2022.

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

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bonn, 11 March 2025

The Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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 IT product identified in this report was assessed according to the procedures on Assurance Continuity [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 SMGW, Version 2.0, Power Plus Communications AG, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [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 certified product itself did not change.

The changes are related to the certified scope of the delivery procedures. The assurance component ALC_DEL.1 (ALC_DEL.1.1D, ALC_DEL.1.1C) has been refined in the ST [4] to only cover the delivery of the TOE from the manufacturer to the MPO (metering point operator), who is the customer of the developer and the recipient of the TOE.
The further storage and transport of the TOE to the installation environment falls into the responsibility of the MPO and is out of scope of the CC certification.
A related assumption and corresponding security objective for the TOE environment have been added to the ST [4].

Conclusion

The maintained change is at the level of the delivery procedures. The change has no effect on product assurance, but the updated guidance documentation [6] has to be followed.

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-0831-V5-2022 dated 20 December 2022 updated by a re-assessment [5] on 18 December 2024 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 BSIG[1] Section 9, Para. 4, Clause 2).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

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 3.1, 29 February 2024

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.2, March 2024

[2] Impact Analysis Report, Version 1.0, 24 October 2024, Power Plus Communications AG (confidential document)

[3] Certification Report BSI-DSZ-CC-0831-V5-2022 for SMGW, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik, 20 December 2022

[4] Security Target SMGW, Version 2.0, Version 5.6, 09 January 2025, Power Plus Communications AG

[5] Assurance Continuity Reassessment Report BSI-DSZ-CC-0831-V5-2022-RA-01 for SMGW, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik, 18 December 2024

[6] Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung, Version 1.15, 02 December 2024, Power Plus Communications AG