Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0831-V3-2021-MA-01

SMGW Version 1.1.2

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 *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-0831-V3-2021.

The change to the certified product is at the level of a minor, non-security relevant adaption in the implementation representation and an additional communication adapter (non-TOE). The identification of the maintained product is indicated by a new version number compared to the certified product.
Additionally, the life cycle security aspect ALC_DEL was updated to consider changes in the delivery procedure.

Consideration of 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-V3-2021 dated 12 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-0831-V3-2021.

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

Bonn, 30 March 2021

The Federal Office for Information Security

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - 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 *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 [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the SMGW Version 1.1.2, Power Plus Communications AG, 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 SMGW Version 1.1.2 was changed to improve the TOE internal operating system routines and to include a new (TOE external) communication adapter. Configuration Management procedures required a change in the product identifier. Therefore the version number changed from Version 1.1.1 (SW version 32222-32349) to Version 1.1.2 (SW version 32474-32475).
Furthermore, the hardware revision number engraved on the SMGW case is extended to consider the new communication adapter. The revision number follows the following structure: “SMGW-X-YY-111-n0”. Here, the X represents the communication variant (E=Ethernet, P=powerWAN Ethernet, B=BPL, G=GPRS, L=LTE, C=CDMA, N=G.hn). For more details see Security Target [5], chapter 1.2.

The Security Target [5] and the guidance documentation [9] – [11] were editorially updated.

Additional changes are related to an update of life cycle security aspect ALC_DEL. The ALC re-evaluation was performed by the ITSEF TÜV Informationstechnik GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [6]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [5].

The new documentation of the delivery procedures [8] replaces the old version [7].

Conclusion

The maintained change is at the level of a minor, non-security relevant adaption in the implementation representation and an additional communication adapter (non-TOE). The identification of the maintained product is indicated by a new version number compared to the certified product.
Additionally, the life cycle security aspect ALC_DEL was updated to consider changes in the delivery procedure. The change has no effect on product assurance, but the updated guidance documentation has to be followed.

Consideration of 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-V3-2021 dated 12 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 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 2.1, June 2012

[2] Impact Analysis Report, Maintenance-Verfahren zur Anpassung der Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung, SMGW Version 1.1.2, Version 1.5, 08 March 2021, OpenLimit SignCubes GmbH, Power Plus Communications AG (confidential document)

[3] Certification Report BSI-DSZ-CC-0831-V3-2021 for SMGW Version 1.1.1, 12 March 2021, Federal Office for Information Security, Germany

[4] Security Target BSI-DSZ-CC-0831-V3-2021, Version 4.6, 02 February 2021, Security Target SMGW Version 1.1.1, OpenLimit SignCubes GmbH, Power Plus Communications AG

[5] Security Target BSI-DSZ-CC-0831-V3-2021-MA-01, Version 4.7, 19 March 2021, Security Target SMGW Version 1.1.2, OpenLimit SignCubes GmbH, Power Plus Communications AG

[6] EVALUATION TECHNICAL REPORT SUMMARY, BSI-DSZ-CC-0831-V3-2021-MA-01, Version 2, 26 March 2021, TÜV Informationstechnik GmbH (confidential document)

[7] Auslieferungs- und Fertigungsprozeduren - Anhang Sichere Auslieferung, Version 1.11, 25 September 2020, OpenLimit SignCubes GmbH, Power Plus Communications AG

[8] Auslieferungs- und Fertigungsprozeduren - Anhang Sichere Auslieferung, Version 1.3, 19 March 2021, OpenLimit SignCubes GmbH, Power Plus Communications AG

SHA-256 hash value:
6fdd2e0850078ee78f5fa51f646fabcb70cad73289066a03717a6195208b1838

[9] Handbuch für Verbraucher, Smart Meter Gateway, Version 4.4, 02 March 2021, OpenLimit SignCubes GmbH, Power Plus Communications AG

SHA-256 hash value:
8488f6be2faad548e487f968a617a426dfcda9025780a7885d13023736878e03

[10] Handbuch für Service-Techniker, Smart Meter Gateway, Version 4.8, 02 March 2021, OpenLimit SignCubes GmbH, Power Plus Communications AG

SHA-256 hash value:
9a614ecf9a424850842a2c8ba1ab9911d6ee2fa4a343ac681288bcbf8183424e

[11] Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, SmartMeter Gateway, Version 4.2, 02 March 2021, OpenLimit SignCubes GmbH, Power Plus Communications AG

SHA-256 hash value:
3a7fb265844f6e94a2f231b7068ab6d5349b864c25e71034ab8affe1a0a7397f