



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0919-2019-MA-01

CASA 1.0

Software Version: 30000000__X026c

Hardware Version: 10 301 / 10 302 / 10 303 / 10 304

from

EMH metering GmbH & Co. KG



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-0919-2019.

The change to the certified product is at the level of security irrelevant changes in the implementation of the tariffing functionality and the introduction of alternatives for existing passive hardware components. The identification of the maintained product is indicated by a new TOE software version number compared to the certified product.

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-0919-2019 dated 17 December 2019 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-0919-2019.

Bonn, 4 June 2020

The Federal Office for Information Security



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



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 CASA1.0, EMH metering GmbH & Co. KG, 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 CASA 1.0 was changed to exclude potential errors in the tariffing functionality and to introduce alternatives for existing passive hardware components. Configuration Management procedures required a change in the product identifier. Therefore the TOE software version number changed from 30000000__X026b to 30000000__X026c.

The Security Target [5] and the guidance documentation [7, 8] were editorially updated.

Conclusion

The maintained change is at the level of security irrelevant changes in the implementation of the tariffing functionality and the introduction of alternatives for existing passive hardware components. The change has no effect on product assurance.

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-0919-2019 dated 17 December 2019 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).

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] CASA 1.0 Maintenance-Verfahren 001 Impact Analysis Report (IAR), Version 0.04, 08 April 2020, EMH metering GmbH & Co. KG (confidential document)
- [3] Certification Report BSI-DSZ-CC-0919-2019 for CASA 1.0, 17 December 2019, Federal Office for Information Security
- [4] CASA 1.0 Security Target, Version 2.00, 16 December 2019, EMH metering GmbH & Co. KG
- [5] CASA 1.0 Security Target (CASA-ST), Version 2.01, 23 March 2020, EMH metering GmbH & Co. KG
- [6] CASA 1.0 Konfigurationsliste, Version 10, 17 April 2020, EMH metering GmbH & Co. KG (confidential document)
- [7] CASA 1.0 (CASA-AGD) Benutzerhandbuch für Letztverbraucher, Version 1.18, 20 March 2020, EMH metering GmbH & Co. KG
- [8] CASA 1.0 (CASA-AGD) Installations- und Konfigurationshandbuch für Service-Techniker und Gateway-Administratoren, Version 1.18, 20 March 2020, EMH metering GmbH & Co. KG