



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0918-V5-2023-MA-01

**CONEXA 3.0 Version 1.4, Software: v3.67.0-cc,
Hardware: HW V01.00**

from

Theben 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-0918-V5-2023.



The change to the certified product is at the level of the secure delivery procedure. The certified product itself did not change. The changes are related to an update of the user guidance and an update of life cycle security aspects.

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.



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

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-0918-V5-2023 dated 11. May 2023 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-0918-V5-2023.



Bonn, 9 June 2023

The Federal Office for Information Security

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 CONEXA 3.0 Version 1.4, Software: v3.67.0-cc, Hardware: HW V01.00, Theben 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 CONEXA 3.0 Version 1.4, Software: v3.67.0-cc, Hardware: HW V01.00 was changed due to a new version of the secure delivery procedure.

The certified product itself did not change.

The changes are related to an update of the user guidance [5] and [6] only. Other existing guidance documents remain valid. The description of the secure delivery procedure was extended due to adding an alternative delivery procedure (cardbox delivery).

The changes are related to an update of life cycle security aspects. The ALC_DEL re-evaluation was performed by TÜV Informationstechnik GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [7]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

Conclusion

The maintained change is at the level of life cycle security aspects. The change has no effect on product assurance, but the updated guidance documentation 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-0918-V5-2023 dated 11. May 2023 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 2.2, 30 September 2021
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.0, November 2019
- [2] Impact Analysis Report, V0.5, 11.04.2023, Theben AG (confidential document)
- [3] Certification Report BSI-DSZ-CC-0918-V5-2023 for CONEXA 3.0 Version 1.4, 11.05.2023, Bundesamt für Sicherheit in der Informationstechnik
- [4] Security Target CONEXA 3.0 - Smart Meter Gateway, Version 1.94,2, 07.10.2022, Theben AG
- [5] Prozesshandbuch theSi - Für den Einsatz von Kartonage Verpackungen in Sicherer Lieferkette im Projekt Smart Metering, Version 0.6, 02.02.2023, Theben AG
- [6] Anhang sichere Auslieferung Smart Meter Gateway Conexa 3.0, Version 0.14, 28.11.2022, Theben AG
- [7] Evaluation Technical Report (ETR Summary), Version 1, 05.06.2023, TÜV Informationstechnik GmbH (confidential document)