

# Assurance Continuity Reassessment Report

**BSI-DSZ-CC-0918-V6-2024-RA-01**

**CONEXA 3.0 Version 1.5**

**(Software: v3.80.0-cc / Hardware: HW V01.00 & V01.01, gemäß BSI-DSZ-CC-0918-V6-2024-MA-03)**

**(Software: v3.80.3-cc / Hardware: HW V01.00 & V01.01, gemäß BSI-DSZ-CC-0918-V6-2024-MA-02)**

from

**Theben Smart Energy GmbH**



SOGIS  
Recognition Agreement  
for components up to  
EAL 4

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-0918-V6-2024 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-0918-V6-2024.



Common Criteria  
Recognition  
Arrangement  
recognition for  
components up to EAL  
2 and ALC\_FLR only

Bonn, 12 January 2026

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 applied regarding cryptographic security functionality. The previous certification report [6] still applies in that regard.

### Regarding assurance class life cycle (ALC):

No changes applied to the assurance aspect ALC. The previous certification report [6] still applies 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] 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 TOE<sup>1</sup> <https://www.bsi.bund.de/AIS>
- [5] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 3.0, March 2023,  
Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.1, June 2023
- [6] Certification Report BSI-DSZ-CC-0918-V6-2024 for CONEXA 3.0 SW: v3.80.0-cc, HW V01.00 & V01.01, Bundesamt für Sicherheit in der Informationstechnik, 08.02.2024  
amended by the following Assurance Maintenance Reports:  
BSI-DSZ-CC-0918-V6-2024-MA-01, 19.04.2024  
BSI-DSZ-CC-0918-V6-2024-MA-02, 29.01.2025  
BSI-DSZ-CC-0918-V6-2024-MA-03, 29.01.2025
- [7] Security Target (ASE) CONEXA 3.0 - Smart Meter Gateway, Version 1.96.2, 04.12.2024, Theben Smart Energy GmbH
- [8] Evaluation Technical Report Summary, Version 1, 05.12.2025, TÜV Informationstechnik GmbH (confidential document)

1 specifically

- [AIS1] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers,
- [AIS14] *Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)*
- [AIS19] *Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)*
- [AIS23] *Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler,*
- [AIS32] *Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema*
- [AIS41] *Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for PPs and STs*
- [AIS46] *Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren*