Federal Office
for Information Security

Certification Report

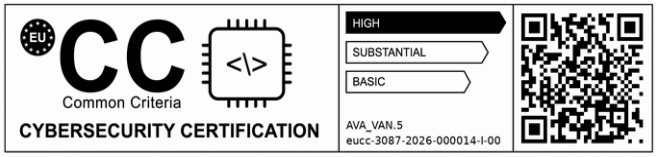
EUCC-3087-2026-0014
Administration ID
BSI-DSZ-CC-0918-V9-2026

for

CONEXA 3.0 Version 1.8 Software: v3.90.0-cc,
Hardware: HW V01.00 & V01.01 & V01.02

from

Theben Smart Energy GmbH



BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-11

Contents

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 as published on the day of issuance of this certificate and as mirrored by the Common Criteria for IT Security Evaluation (CC), Version CC:2022 [CC]
- ISO/IEC 18045 as published on the day of issuance of this certificate and as mirrored by the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Recognition Agreements

In order to avoid multiple certifications of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed

3.1. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- The TOE CONEXA 3.0 Version 1.8, Software: v3.90.0-cc, Hardware: HW V01.00 & V01.01 & V01.02 has been re-certified by the certification body of the Federal Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-0918-V8-2025. Specific results from the evaluation process were re-used.
- The evaluation of the product CONEXA 3.0 Version 1.8, Software: v3.90.0-cc, Hardware: HW V01.00 & V01.01 & V01.02 was carried out by
  TÜV Informationstechnik GmbH, located at
  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 30 July 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).
- This certification was applied for: Theben Smart Energy GmbH.
- The assessed TOE was developed by: Theben Smart Energy GmbH.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

- all statements and indications regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in an environment as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be reassessed. Therefore, the holder of the certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a reassessment on a regular e.g. annual basis.

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 31 July 2026 is valid until 30 July 2034 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

1. to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures,
2. to monitor the resistance of the certified product against new attack methods and to provide a qualified confirmation by applying for a re-certification or re-assessment

process on a regular basis every two years starting from the issuance of the certificate.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme's assurance continuity (i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE CONEXA 3.0 Version 1.8, Software: v3.90.0-cc, Hardware: HW V01.00 & V01.01 & V01.02 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[5] Theben Smart Energy GmbH
Schlossfeld 9
72401 Haigerloch

B. Certification Results

The following chapters summarise the assessment results of the

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Executive Summary

The Target of Evaluation (TOE) presented in this document is called "Smart Meter Gateway", “SMGW” or “Gateway” and uniquely identified as CONEXA 3.0 (CC), Version 1.8. It is the communication unit used within such an intelligent metering system and represented by the product CONEXA 3.0 except for the integrated Security Module.

Besides data processing, Smart Meter Gateway offers possibility to generate tariff rates in order to enable network operators and consumers to control energy consumption in an intelligent way.

The product CONEXA 3.0 Version 1.8, Software: v3.90.0-cc, Hardware: HW V01.00 & V01.01 & V01.02 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a re-certification based on BSI-DSZ-CC-0918-V8-2025 (BSI administration ID). Specific results from the evaluation process BSI-DSZ-CC-0918-V8-2025 (BSI administration ID) were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product CONEXA 3.0 Version 1.8, Software: v3.90.0-cc, Hardware: HW V01.00 & V01.01 & V01.02 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 30 July 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO], [EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014 [PP]
- Assurance Level: EUCC High with component AVA_VAN.5
- Assurance Package: EAL 4
- Augmentation: ALC_FLR.2 and AVA_VAN.5

The Security Target [ST] is the basis for this certification. It is based on the certified Protection Profile Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014 [PP].

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitely guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology product is identified as follows:

CONEXA 3.0 Version 1.8, Software: v3.90.0-cc, Hardware: HW V01.00 & V01.01 & V01.02

Holder of the certificate: Theben Smart Energy GmbH
Schlossfeld 9
72401 Haigerloch
https://www.theben-se.de/conexa

The following table outlines the TOE deliverables (all Hashsums SHA256 values):

No	Type	Identifier	Release	Form of Delivery
1	HW	CONEXA 3.0	HW V01.00 HW V01.01 HW V01.02	Secure Delivery Procedure via transport service and installation by a service technician or personal hand over
2	SW	SMGW Software	v3.90.0-cc	Pre-Installed on the HW
3	DOC	Handbuch CONEXA 3.0 für den Gateway Administrator [AGD_GWA]	v2.15.0 afc6c06102d34f09aa4ebf9f5417f5e5c84a a8061a0eafec46e463c4ef915e8c	Download from https secured website
4	DOC	Handbuch CONEXA 3.0 für den Service-Techniker [AGD_SRV]	v2.16.2 769b7b7dbf510efdbe157d5175ea1ad479 cdfe8c2ee55f461ca6406c01920cbb	Download from https secured website
5	DOC	Handbuch CONEXA 3.0 für den Letztver-braucher [AGD_LV]	v2.14.2 3101bd767aaf2cb2f3c19366b7a1fe6a10 90704bdd96bd0e6827276e12fce46b	Download from https secured website
6	DOC	Conexa 3.0 Profilbe-schreibungen [CON_PROF]	v2.18 0e55586bf1a34feeab1d3c5ab765685c8a 1e1885e07a2762864000255672d9ed	Download from https secured website
7	DOC	COSEM HTTP-Webservice [COSEM]	v2.2 8ababcaff546dbfc060d0100bd2fd6a5b99 988af99d9b97c759b22626dea8dd	Download from https secured website
8	DOC	Conexa 3.0 Logmeldungen [CON_LOG]	1.13.1 ce67376730aa8316758e1b54e43a1bbaf 81e3f819fc20dbd3eac5c7dd1baed60	Download from https secured website
9	DOC	Schnittstellenbe-schreibung [IF_GW_CON]	v1.4 26c821592d7245e29ce91fc25c5dacc0c3 310f2885fa9e1baff30d7e97103221	Download from https secured website
10	DOC	Schnittstellenbe-schreibung [IF_GW_SRV]	v1.4 ec094d7ff046c387e921bfdd2d494433083 030745cc22cdf20824dc5f5feab99	Download from https secured website
11	DOC	Anhang sichere Auslieferung [MPO]	V0.16 ab5c8b7ca02ec838fccd22c6ec00c0bdaf0 de43dff0de0e08c9ebbfe70f435c2	Download from https secured website

Table 1: Deliverables of the TOE

With the introduction of the MPO delivery chain [MPO], the definition of responsibility for SMGW delivery methods was sharpened as follows:

- The TOE developer is responsible for the secure development, production and delivery to the MPO.
- Upon acceptance of the TOE from the developer, the respective MPO takes over responsibility for the subsequent storage, transport and assembly of the TOE.

This definition was announced by the BSI by publishing the possibility of the MPO delivery chain which was taken over by the developer. As already explained reduces the integration of the MPO delivery the scope of the certification. Only the delivery of the TOE from the developer to the MPO is part of this certification.

The TOE thereby consists of the main circuit board of the Smart Meter Gateway, the case and the seal. The correct hardware of the TOE can be identified by the identifier “HW V01.00”, “HW V01.01” or “HW V01.02”, which can be found on a laser engraving on the TOE.

The firmware and software are pre-installed on the hardware and therefore also part of the physical delivery. It can be uniquely identified by all users by connecting to the TOE and using the commands described in the relevant guidance document.

The guidance documents mentioned in Table 1 can be downloaded by a https secured website. The corresponding users can uniquely identify the guidance by checking the hash sum, which is also included in the Security Target.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

Security Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Privacy, Protection of the TSF, and Trusted Path/Channels.

Specific details concerning the above mentioned security policies can be found in Chapter 6 of the Security Target [ST].

A reference and description of the vulnerability handling policy and the assurance continuity policy can be found here: https://www.theben-se.de/conexa/cyber-security-info

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These uncovered aspects need to be provided for by specific security objectives that have to be met by the TOE environment. They are in particular:

OE.ExternalPrivacy: Authorised and authenticated external entities receiving any kind of private or billing-relevant data shall be trustworthy and not perform unauthorised analyses of these data with respect to the corresponding Consumer(s).

OE.TrustedAdmins: The Gateway Administrator and the Service Technician shall be trustworthy and well-trained.

OE.PhysicalProtection: The TOE shall be installed in a non-public environment within the premises of the consumer that provides a basic level of physical protection. This protection shall cover the TOE, the Meters that the TOE communicates with and the communication channel between the TOE and its Security Module. Only authorised individuals may physically access the TOE.

OE.Profile: The Processing Profiles that are used when handling data shall be obtained from a trustworthy and reliable source only.

OE.SM: The environment shall provide the services of a certified Security Module for

- Verification of digital signatures,
- Generation of digital signatures,
- Key agreement,
- Key transport,
- Key storage, and
- Random Number Generation.

The Security Module used shall be certified according to [SM-PP] and shall be used in accordance with its relevant guidance documentation.

OE.Update: The firmware updates for the Gateway that can be provided by an authorised external entity shall undergo a certification process according to this Security Target before they are issued to show that the update is implemented correctly. The external entity that is authorised to provide the update shall be trustworthy and ensure that no malware is introduced via a firmware update.

OE.Network: It shall be ensured that

- a WAN network connection with sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,
- the Gateway is the only communication gateway for Meters in the LMN, and
- if devices in the HAN have a separate connection to parties in the WAN (be-side the Gateway) this connection is appropriately protected.

OE.Keygen: It shall be ensured that the ECC key pair for a Meter (TLS) is generated securely according to the [BSI-TR-03109-3]. It shall also be ensured that the keys are brought into the Gateway in a secure way by the Gateway Administrator.

OE.Delivery: After the reception of the TOE by the MPO, the MPO is responsible for the secure delivery of the TOE to the installation and operational environment. The MPO shall be trustworthy in context of this delivery and well trained and shall take appropriate security measures to ensure protection against undetected manipulation or undetected replacement of the TOE during such a delivery to ensure integrity and authenticity of the TOE. Note that adhering to [MSB-Katalog] is sufficient for MPOs to fulfill this security objective.

Details can be found in the Security Target [ST].

5. Architectural Information

The TOE is subdivided into the following subsystems:

- Hardware: Includes the case of the SMGW, the seals and the electronic parts of the TOE and provides the physical basis as well as the passive physical protection for the TOE.
- OS: Includes the underlying operating system and provides the filesystem encryption, firewall functionality and mandatory access control.
- SMPF: Implements parts of the SMGW software and provides the functionality for system initialisation after the boot process, authentication of external entities, management of processing profiles and logging.
- Crypto: Implements parts of the SMGW software and provides the cryptographic functions of the TOE and the interface to the Security Module.
- Services: Implements parts of the SMGW software and provides the webserver for the requests send by the gateway administrator, service technician and consumer
- WAN: Implements parts of the SMGW software and provides the wake-up-service, the communication channels for the GWA and the external entities.
- HAN: Implements parts of the SMGW software and provides the communication channels to the external entities at the HAN interface.
- Calibration: Implements parts of the SMGW software and provides the communication channels to the meters at the LMN interface as well as the processing of the received meter data.

6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Period of support:

Theben Smart Energy GmbH provides support for CONEXA 3.0 at least for the entire period of validity of the applicable CC certificate of the respective product version. Security advisories and security updates are provided during this period.

Contact information and accepted reporting methods:

E-mail address for security-related reports: zertifizierungen@theben-se.de. Reports should be sent PGP-encrypted. PGP fingerprint: 548F 15FF 1A3F 2EB2 2BDE 4F48 0729 0B74 62D7 04F6. The corresponding public key is available for download on the page. The reporting channel is open to end users and to external security researchers.

Vulnerability repositories and advisories:

Theben Smart Energy GmbH continuously assesses vulnerability information relating to CONEXA 3.0, including publicly disclosed vulnerabilities in third-party components used. Where a vulnerability is assessed as relevant to the product, Theben Smart Energy GmbH issues a security advisory. Advisories containing technical details, affected product versions and recommended actions are made available to the affected metering point operators via the customer portal. This restriction serves coordinated disclosure and the protection of the installed base; it is not tied to a paid option. Published advisories are listed with identifier, date, affected product version, severity (CVSS), assigned CVE ID where applicable, and status. At present, no publicly disclosed vulnerabilities are known for CONEXA 3.0. Publicly disclosed vulnerabilities relating to the product and to the third-party

components used can be researched via the National Vulnerability Database (NVD) / CVE Program and via the BSI advisory service (CERT-Bund).

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

All tests have been carried out by ITSEF:

TÜV Informationstechnik GmbH,
Unternehmensgruppe TÜV NORD
Am TÜV 1
45307 Essen
under the responsibility of certification Body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 for details on assurance levels or packages involved into testing.

The evaluation was realised in accordance with [CC], while considering [CEM] and [CC_ERR].

Additionally, the following interpretations are considered:

Interpretations of AIS 1, AIS 14, AIS 19, AIS 32, AIS 34, AIS 46 and AIS 48 [AIS] are considered.

Additionally, the interpretations, CC Supporting Mandatory Technical Documents and CC Supporting Guidance Documents are considered.

The following State-of-the-art-documents were applied:

All state-of-the-art documents and guidelines for EUCC are applied. The EUCC regulations were complemented by JIL guidelines and AIS scheme interpretations in case no equivalent EUCC regulation is available.

There is only one final TOE configuration, which was tested. Nevertheless, the developer also provided an additional modification including SSH access for a minor set of testing.

Developer Testing

The developer’s testing approach was to test the TSFI systematically next to a deeper consideration of TOE subsystems, internal interactions and concrete SFR tests. In order to do this, the developer tests were produced during the development of the TOE, to sufficiently cover the TSF. The coverage and depth in testing all SFRs, TSFIs as well as the TOE behaviour and existing interactions on level of subsystems were also summarized by the developer and evaluated by the evaluation body without relevant deviations.

The developer’s testing effort has been proven sufficient to demonstrate that the security functionality / TSFI perform as specified and has therefore passed the evaluator’s examination.

Independent Testing

The evaluation body used the same TOE variants, test configurations and test environment as the developer during functional testing (also final and SSH variant and

always IPv4 stack). Additionally, the evaluation body used an independent test system (Exceeding Solutions) to perform the independent tests of the ITSEF.

The tested TOE (SW version v3.88.28 and v3.88.29) is consistent with the version under evaluation as specified in [ST] (SW version v3.90.0-cc). The ITSEF verified that neither the TOE behaviour, nor any further security-relevant effects might result by the performed source code adaptions.

The overall test result is that no deviations were found between the expected and the actual test results.

Penetration Testing

The evaluation body conducted penetration testing based on functional areas of concern derived from SFRs and architectural mechanisms. These areas were prioritized with regard to various factors, e.g. attack surface, estimated flaw likelihood, developer testing coverage and detectability of flaws during developer testing.

Medium and high areas were guaranteed to be penetration tested with a stronger emphasis on high priorities. Low priorities were also considered during penetration, but could be less emphasized if developer tests were found to be sufficient.

The penetration testing activities were performed as tests and as analytical tasks. Whenever an analysis was estimated to yield better results, the evaluators chose the analytical approach. Analytical activities were especially applied in the areas secure boot, self-protection, domain separation, kernel and system hardening as well as non-bypassability. Combined approaches were also applied.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment provided that all measures required by the developer are applied.

Please refer to chapter 11 for complete and precise information on settings and configuration of the TOE during the evaluation, including relevant operational notes and observations.

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

Hardware:

The main circuit board of the TOE is built into a sealed case of the complete product (Smart Meter Gateway) and can be identified by the laser engraving on the case showing a hardware vision number. The delivered TOE hardware has the hardware version HW V01.00, HW V01.01 or HW V01.02. As a further authenticity feature, a cross-developer identification is present at the casing (next to the HW identifier, always starting with "E THE 03" followed by eight more digits).

Firmware/Software:

The installed software version can be checked by all different user roles. Summarized, the identification of the software can be done as following:

Part	Consumer	Service Technician	Gateway Administrator
Software Version:	Software version can be displayed via	Software version can be displayed via Service-	Software version can be requested with a statistic

v3.90.0-cc	consumer browser interface.	Techniker-Tool or an alternative REST client.	profile via management channel.

Guidance Documents:

The Guidance documentation can be uniquely identified by checking the hash value of the files against the hash sum stated in the Security Target [ST].

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports (ETR) [ETR] according to the the requirements of the Scheme [EUCC-VO], [EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

On advise by the Certification Body and consent by the certificate holder the following guidance further specific for the technology of the product [AIS], (AIS 34) was applied:

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE. The corresponding TOE is identified in chapter 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0014, administration ID BSI-DSZ-CC-0918-V9-2026
- was issued on: 31 July 2026
- is valid until: 30 July 2034

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
TLS cipher suite (key establishment, record layer encryption and integrity, peer authentication)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_EC-	Cipher Suite: [RFC 5289], [RFC 5246] AES: [FIPS 197] CBC: [NIST SP800-38A] HMAC: [RFC 2104] GCM: [NIST SP800-38D] brainpoolPxxxr1: [RFC 5639]	AES: 128bit, 256bit EC: secp256r1, secp384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	[TR03109]	2029+

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
	DSA_WITH_AES_256_GCM_SHA384	secpxxxr1: [RFC 5114] SHA: [FIPS 180-4]			
Key generation for CMS containers	Key generation: ECKA-EG Key wrap: id-aes128-wrap	Key wrap: [RFC 3394] Key generation: [TR 03111]	128bit	[TR03109]	2029+
Encryption / decryption /integrity of CMS container	id-aes128-gcm, id-aes-CBC-CMAC-128	CMAC: [RFC 4493] GCM: [RFC 5084], [NIST SP800-38D] AES: [FIPS 197] CBC: [NIST SP800-38A]	128bit	[TR03109]	2029+
Key generation for meter data	AES-CMAC	AES-CMAC: [RFC 4493] AES: [FIPS 197]	128bit	[TR03109]	2029+
Encryption/decryption, integrity of meter data	Encryption: AES-CBC Integrity protection: AES-CMAC	AES-CMAC: [RFC 4493] AES: [FIPS 197] CBC: [NIST SP800-38A]	128bit	[TR03109]	2029+
Hashing for signatures	SHA-256, SHA-384, SHA-512	SHA: [FIPS 180-4]	-	[TR-02102]	2029+
Encryption / decryption, integrity of TSFI	AES-128-CBC ES-SIV:SHA256	AES: [FIPS 197] CBC: [NIST SP800-38A] SHA: [FIPS 180-4]	128bit	[TR-02102]	2029+
Remarks	Integrity of firmware updates and stored binaries of TSFI are not defined in SFRs per ST but they are implemented as ARC mechanisms. They have been evaluated.				

Table 2: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2).

According to [TR03116] or [TR02102] respectively, the algorithms are suitable for Smart Metering Systems. The validity period of each algorithm is mentioned in the official catalogue [TR02102].

10. Obligations and Notes for the Usage of the TOE

Table 1: Deliverables of the TOE outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition all aspects of

Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

The customer or user of the TOE shall take the statements of this certificate into account in its system risk management process. The user should define measures in its risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been reassessed.

The user also has to consider in its risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. Until the TOE has been re-certified, the user should examine the use of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [ST] of the TOE / Information and communications technology (ICT) product is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None.

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLS	Controllable Local Systems
CMS	Cryptographic Message Syntax
CMAC	Cipher-Based Message Authentication Code
CMS	Cryptographic Message Syntax
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
GCM	Galois/Counter Mode
GWA	Gateway Administrator

HAN	Home Area Network
HMAC	Keyed- Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and communications technology
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LMN	Local Metrological Network
LTE	Long Term Evolution
MAC	Message Authentication Code
NTP	Network Time Protocol
PP	Protection Profile
OS	Operation System
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
SHA	Secure Hash Algorithm
SMGW	Smart Meter Gateway
SMPF	Smart Metering Platform Framework
SSH	Secure Shell
ST	Security Target
TAF	Tarifanwendungsfall
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAN	Wide Area Network

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
and
Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC] ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html
as mirrored by CCRA's edition:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities

- Part 5: Pre-defined packages of security requirements
https://www.commoncriteriaportal.org

[CEM] ISO 18045:2022: Information Technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

as mirrored by CCRA's edition:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[CC_ERR] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15, CCMB-2025-001

[EUCC_SOTA] EUCC state-of-the-art documents:
https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en

[EUCC_PROG] EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), https://www.bsi.bund.de/zertifizierung

[EUCC_CERT] EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/) but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)

[AIS] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6] https://www.bsi.bund.de/AIS

[ST] Security Target (ASE) CONEXA 3.0 - Smart Meter Gateway, BSI-DSZ-CC-0918-V9-2026, Version 1.99.5, 2026-07-14, Theben Smart Energy GmbH

[PP] Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014

[IAR] Impact Analysis Report – Smart Meter Gateway CONEXA, Version 0.9, 2026-05-29, Theben Smart Energy GmbH (confidential document)

[ETR] Evaluation Technical Report, Version 1, 2026-07-27, TÜV Informationstechnik GmbH, (confidential document)

[Conflist_HW] ALC_CMS.4 Konfigurationsliste Smart Meter Gateway CONEXA 3.0, 1.0 Theben Smart Energy GmbH (confidential document)

[Conflist_SW] Assurance Life Cycle – Configuration Management der CONEXA 3.0, V3.90.0-cc, Theben Smart Energy GmbH (confidential document)

[6]specifically

- AIS1 Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14
- AIS14 Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7
- AIS19 Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 46 Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3
- AIS 48 Anforderungen an die Prüfung von Sicherheitsetiketten, Version 1.0

[AGD_GWA] Handbuch CONEXA 3.0 für Gateway Administrator, 2.15.0, 2026-02-02 Theben Smart Energy GmbH

[AGD_LV] Handbuch CONEXA 3.0 für den Letztverbraucher, 2.14.2, 2026-07-02 Theben Smart Energy GmbH

[AGD_SRV] Handbuch CONEXA 3.0 für den Service-Techniker, 2.16.2, 2026-07-02 Theben Smart Energy GmbH

[CON_LOG] Logbucheinträge CONEXA 3.0 – Smart Meter Gateway, 1.13.1,2026-04-15 Theben Smart Energy GmbH

[CON_PROF] Profilbeschreibungen CONEXA 3.0 Smart Meter Gateway, 2.18, 2026-01-22, Theben Smart Energy GmbH

[COSEM] COSEM HTTP-Webservice, Version 2.2, Theben Smart Energy GmbH

[IF_GW_CON] Schnittstellenbeschreibung IF_GW_CON, Version 1.4, Theben Smart Energy GmbH

[IF_GW_SRV] Schnittstellenbeschreibung IF_GW_SRV, Version 1.4, Theben Smart Energy GmbH

[MPO] Anhang sichere Auslieferung CONEXA 3.0 Smart Meter Gateway, 0.16, Theben Smart Energy GmbH

[SiLKe] BSI. Anforderungskatalog zur MSB-Lieferkette, in der aktuell gültigen Fassung. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/MSB/MSB_node.html (cit. on pp. 38, 47). 2024, German Federal Office for Information Security

[TR] Technische Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnik):
TR-03109-1, Anlage IV, Feinspezifikation „Drahtlose LMN-Schnittstelle“, Teil a: „OMS Specification Volume 2, 13.12.2024, Primary Communication“, Version 2.0
TR-03109-1, Anlage IV, Feinspezifikation „Drahtgebundene LMN-Schnittstelle“, Teil a: „HDLC für LMN“, Version 2.0, 13.12.2024
TR-03109-1, Anlage IV, Feinspezifikation „Drahtgebundene LMN-Schnittstelle“, Teil b: „SML-Smart Message Language“, Version 2.0, 13.12.2024
TR-03109-3: Technische Richtlinie BSI-TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, BSI, Version 1.1, 2014
TR-02102 Technische Richtlinie TR-02102 “Kryptographische Verfahren: Empfehlungen und Schlüssellängen”:
TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2025-01,
TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2025-01
TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2025-01
BSI-TR-03116-3, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme, Stand 2025, German Federal Office for Information Security, 13.12.2024.
TR-03111: Elliptic Curve Cryptography (ECC). Version 2.10, 01.06.2018

[Standard] [FIPS 180-4] NIST FIPS PUB 180-4: Secure Hash Standard (SHS). NIST, August 2015.

[FIPS 197] NIST FIPS PUB 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2023-05-09, NIST, 2023.
[NIST SP800-38A] NIST SP800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST, 2001.
[NIST SP800-38B] NIST SP800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. NIST, 2005.
[NIST SP800-38D] NIST SP800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST, 2007.
[RFC 2104] Network Working Group RFC 2104, H. Krawczyk et al.: HMAC: Keyed- Hashing for Message Authentication. Network Working Group, Feb. 1997.
[RFC 3394] IETF RFC 3394, J. Schaad, R. Housley: Advanced Encryption Standard (AES) Key Wrap Algorithm. IETF, 2002.[RFC 4493] IETF RFC 4493, J. H. Song, J. Lee, T. Iwata: The AES-CMAC Algorithm. IETF, 2006.
[RFC 5084] IETF RFC 5084, R. Housley: Using AES-CCM amd AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS). IETF, 2007.
[RFC 5114] IETF RFC 5114, M. Lepinski, S. Kent: Additional Diffie-Hellman Groups for Use with IETFStandards, 2008
[RFC 5246] RFC 5246 - The Transport Layer Security (TLS) Protocol, Version 1.2, Dierks & Rescorla - Standard Track, August 2008
[RFC 5289] IETF RFC 5289, E. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM). IETF, 2008.
[RFC 5639] IETF RFC 5639, M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. IETF, 2010.....

C. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report