Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0918-V7-2025

for

CONEXA 3.0 Version 1.6

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 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0918-V7-2025 (*)

Smart Meter Gateway

CONEXA 3.0, Version 1.6
Software: v3.85.0-cc
Hardware: HW V01.00 & V01.01

from	Theben Smart Energy GmbH
PP Conformance:	Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2, AVA_VAN.5
valid until:	5 February 2033

SOGIS
Recognition Agreement
for components up to
EAL 4

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

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

Bonn, 6 February 2025

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. 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 conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] 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

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

3. Recognition Agreements

In order to avoid multiple certification 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. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it 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 SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

3.2. 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 3 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product CONEXA 3.0, Version 1.6 Software: v3.85.0-cc, Hardware: HW V01.00 & V01.01 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0918-V6-2024. Specific results from the evaluation process BSI-DSZ-CC-0918-V6-2024 were re-used.

The evaluation of the product CONEXA 3.0, Version 1.6 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 31 January 2025. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.
For this certification procedure the applicant is: Theben Smart Energy GmbH.
The product was developed by: Theben Smart Energy GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, 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 Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are 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 re-assessment on a regular e.g. annual basis.
In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 6 February 2025 is valid until 5 February 2033 Validity can be re-newed by re-certification.
The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination

[5] Information Technology Security Evaluation Facility

rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

4. to monitor the resistance of the certified product against new attack methods and to provide a qualified positive confirmation by applying for a recertification or reassessment process on a regular basis every two years starting from the issuance of the certificate.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product CONEXA 3.0, Version 1.6 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Theben Smart Energy GmbH
Schlossfeld 9
72401 Haigerloch
Deutschland

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of 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 1.6. 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 Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1-6.10. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF.AU: Audit	The TOE maintains three kinds of logs: • System Log, • Consumer Log, and • Calibration Log. The purpose of the System Log is to inform the Gateway Administrator and the Service Technician about the system status of Smart Meter Gateway. The Consumer Log informs authorized consumers about all information flows to the WAN, available Processing Profiles, billing relevant and other Meter Data. Within the Calibration Log only calibration-relevant information is stored.
SF.CR: Cryptography	All connections between the TOE and external entities in WAN, HAN or LMN shall be cryptographically protected. Hence, the TOE allows only TLS 1.2 protected connections according to [RFC 5246] between the TOE and entities in the WAN or HAN. For TLS protected connections to the WAN, according to the requirements from [TR 03116-3] the elliptical curve BrainpoolP256r1 is useable only. Thus, the TOE supports the following symmetric cryptographic algorithm: AES-CBC with 128 bit key for encryption and decryption in accordance with [FIPS 197] and [NIST SP800-38A] and AES-CMAC with 128 bit key for integrity protection in accordance to [RFC 4493]. This method enforces that the TOE and the corresponding Meter have a common symmetric 128 bit key.
SF.UD: User Data Protection	The TOE is attached to three separated networks HAN, WAN and LMN. The interfaces to the different networks are physically separated. This TSF controls the access of all external entities in WAN, HAN and LMN to any information that is sent to, from or via the TOE or that is stored within the TOE.
SF.IA: Identification & Authentication	Each user, who communicates with the TOE or receives data from the TOE shall be identified and authenticated before any action on behalf of that user, including receiving of data sent from the Gateway.

TOE Security Functionality	Addressed issue
SF.SM: Security Management	The TOE offers a set of functions to manage and configure the TSF. Those security functions comprise • Management of devices in LMN and HAN, • Client management, • Maintenance of Processing Profiles, • Key- and Certificate-Management, • Firmware Update, • Wake-up configuration, • Monitoring, • Resetting of the TOE (restart), and • Audit Log configuration.
SF.PR: Privacy	This TSF assures the privacy of the Consumer by ensuring that authorized External Entities can only obtain data that is absolutely relevant for billing processes and the secure operation of the grid.
SF.SP: Self-protection	The TOE provides a set of self-protection mechanisms that in particular comprises the self-test of the TOE, detection of replay and physical attacks and the failure with preservation of a secure state.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3-3.5.

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

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

CONEXA 3.0, Version 1.6

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	CONEXA 3.0	HW V01.00 HW V01.01	Secure Delivery Procedure via transport service and installation by a service technician or personal hand over
2	SW	SMGW Software	v3.85.0-cc	Pre-Installed on the HW

No	Type	Identifier	Release	Form of Delivery
3	DOC	Handbuch CONEXA 3.0 für den Gateway Administrator [11]	Version 2.13.3, SHA256 Hash: e3997512641772752d0c600fce2627aa9d78a525d554d3d15e1e26c825fab715	Download from https secured website
4	DOC	Handbuch CONEXA 3.0 für den Service-Techniker [12]	Version 2.14.2, SHA256 Hash: 1e11af36c4135d43a1dba81acaa373025f3f68fa5849a49c2b58add483691b99	Download from https secured website
5	DOC	Handbuch CONEXA 3.0 für den Letztverbraucher [13]	Version 2.12.1, SHA256 Hash: c89a8f8f0324a7e145b3895fb82cfe56d7698bc95a3b3b86236ff41c1d2d4d66	Download from https secured website
6	DOC	Conexa 3.0 Profilbeschreibungen [14]	Version 2.16, SHA256 Hash: 45354f07db962baca72fec33ede98e13697a07d81fa4c28d498ef1fc3e1f7bdc	Download from https secured website
7	DOC	COSEM HTTP-Webservice [16]	Version 2.2, SHA256 Hash: 8abbabcaff546dbfc060d0100bd2fd6a5b99988af99d9b97c759b22626dea8dd	Download from https secured website
8	DOC	Conexa 3.0 Logmeldungen [15]	Version 1.11.0, SHA256 Hash: 88980a569cbfc9d89157248173cdd52be77fec88942f71f8a58c394c04e0309b	Download from https secured website
9	DOC	Schnittstellenbeschreibung IF_GW_CON [17]	Version 1.4, SHA256 Hash: 26c821592d7245e29ce91fc25c5dacc0c3310f2885fa9e1baff30d7e97103221	Download from https secured website
10	DOC	Schnittstellenbeschreibung IF_GW_SRV [18]	Version 1.4, SHA256 Hash: ec094d7ff046c387e921bfdd2d494433083030745cc22cdf20824dc5f5feab99	Download from https secured website
11	DOC	Anhang sichere Auslieferung [19]	Version 0.16, SHA256 Hash: a71d4484abb51133dca17b902a89e6bdc4be5c0fe7c97e93e982b0a1845167bc	Download from https secured website

Table 2: Deliverables of the TOE

As stated earlier, the TOE itself consists of the hardware, firmware and software parts of the Smart Meter Gateway accompanied by the different guidance documents. The physical parts (hardware parts) can be delivered within a special and secure transport box (Pylocx Box) by a standard transportation service, or within a cardboard tamper-detecting packaging with technical support (MVTU) for a small amount of gateways (1 gateway in an individual packaging or an amount of individual packaged gateways packed together in an outer packaging).

The secure transport box can only be opened by authorized individuals by using a special key pad and a valid one time PIN. Due to the mandatory instructions of the developer it is not allowed to remove SMGWs from the secure transport box outside a secure storage room (e.g. at the premise of the energy company) or at the place of installation at the consumers premise where it is installed by a service technician. All places where SMGW will be stored during the delivery need to provide a basic protection against possible attackers (e.g. concrete walls, doors need to be locked, and a physical inventory needs to be performed). Thereby it is ensured that no manipulation of the SMGW can take place on the complete track of delivery (starting with the manufacturer, through the different stages of storages to the final place of installation).

The cardboard packaging may only be opened when the TOE is installed, it is not allowed to remove SMGWs from the secure packaging as they are connected in a special backend. During the whole delivery process the cardboard packaging has to be checked for integrity and verified via a special frontend every time it is stored in a secure storage, left unobserved, or opened for installation. All places where SMGW will be stored during the delivery need to provide basic protection against possible attackers (e.g. concrete walls, doors need to be locked). Thereby it is ensured that no manipulation of the SMGW can take place on the complete track of delivery (starting with the manufacturer, through the different stages of storages to the final place of installation).

All above mentioned delivery variants can be used in order to fulfil the delivery to the MPO. With the introduction of the MPO delivery chain, 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” or “HW V01.01”, 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 2 can be downloaded by a https secured developer’s website. The corresponding users can uniquely identify the guidance by checking the hash sum, which is also included in the Security Target (which will be published on the website of the BSI).

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:

Security audit, communication, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of the TSF and trusted path/ channels.

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 aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

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 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 [24]. 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 [21] is sufficient for MPOs to fulfill this security objective.

Details can be found in the Security Target [6], chapter 4.2.

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. Documentation

The evaluated documentation as outlined in table 2 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.

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

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

7.1. TOE test configuration

All developer tests in the context of the evaluation have been conducted using multiple TOE samples in two different configurations:

- Final TOE with factory setting.
- Instrumentalised TOE with SSH access for TOE manipulations and for firewall tests on the TOE

7.2. 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.

The developer testing covered each TSFI, the case with its seals, the subsystem behaviour and interactions as well as all SFRs.

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

7.3. Independent Evaluator Testing

In summary, all independent and penetration tests were deployed by the ITSEF on the TOE with SW version v3.82.10, which only differs from v3.85.0-cc in minor, not security-relevant adaptations see [20] and in the build process, used certificates (switch from test PKI to live system) and the naming itself. This was evaluated by the ITSEF. Furthermore, all differences between the certified SW version of the TOE during the previous certification (BSI-DSZ-CC-0918-V6) and the actual one under evaluation (BSI-DSZ-CC-0918-V7) were analysed by a detailed source code analyses discussed, without further indication of potential vulnerabilities.

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

7.4. 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.

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.

8. Evaluated Configuration

The TOE as identified in table 2 has been evaluated. There is only one configuration as the different variants of the communication adapters that are outside of the TOE scope run with the same HW and SW configuration of the TOE.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 [4] (AIS 34) and guidance specific for the technology of the product [4] (AIS 46. AIS 48).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2, AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0918-V6-2024, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on adjustment in assignment of counter register to measured value list, introduction resettable firmware only for testing purpose, optimization GWA change process, compression of data at the WAN interface, documentation adaptions, implementation of the MPO delivery method, further changes and bugfixes, kernel update, and editorial changes.

The evaluation has confirmed:

● PP Conformance:	Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014 [8]
● for the Functionality:	PP conformant Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2, AVA_VAN.5

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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_ECDSA_WITH_AES_256_GCM_SHA384	Cipher Suite: [RFC 5289], [RFC 5246] [26] AES: [FIPS 197] [26] CBC: [NIST SP800-38A] [26] HMAC: [RFC 2104] [26] GCM: [NIST SP800-38D] [25] brainpoolPxxxr1: [RFC 5639] [25] secpxxxr1: [RFC 5114] [25] SHA: [FIPS 180-4] [25]	AES: 128bit, 256bit EC: secp256r1, secp384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	[TR03109] [22]	2029+
Key generation for CMS containers	Key generation: ECKA-EG Key wrap: id-aes128-wrap	Key wrap: [RFC 3394] [25] Key generation: [TR 03111] [25]	128bit	[TR03109] [22]	2029+
Encryption / decryption /integrity of CMS container	id-aes128-gcm, id-aes-CBC-CMAC-128	CMAC: [RFC 4493] [25] GCM: [RFC 5084], [25] [NIST SP800-38D] [25] AES: [FIPS 197] [25] CBC: [NIST SP800-38A] [25]	128bit	[TR03109] [22]	2029+
Key generation for meter data	AES-CMAC	AES-CMAC: [RFC 4493] [25] AES: [FIPS 197] [25]	128bit	[TR03109] [22]	2029+
Encryption/ decryption, integrity of meter data	Encryption: AES-CBC Integrity protection: AES-CMAC	AES-CMAC: [RFC 4493] [25] AES: [FIPS 197] [25] CBC: [NIST SP800-38A] [25]	128bit	[TR03109] [22]	2029+
Hashing for signatures	SHA-256, SHA-384, SHA-512	SHA: [FIPS 180-4] [25]	-	[TR-02102] [23]	2029+
Encryption / decryption, integrity of TSFI	AES-128-CBC ES-SIV:SHA256	AES: [FIPS 197] [25] CBC: [NIST SP800-38A] [25] SHA: [FIPS 180-4] [25]	128bit	[TR-02102] [23]	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.				

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).
According to TR-03109-3 [22] or TR-02102-1 [23] the algorithms are suitable for Smart Metering Systems.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs 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 of the TOE is required and thus requested from the sponsor of the certificate.
The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.
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. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage 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 [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AES	Advanced Encryption Standard
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
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLS	Controllable Local Systems
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
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

[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
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0918-V7-2025, Version 1.97.3, 2024-12-02, Security Target (ASE) CONEXA 3.0 - Smart Meter Gateway, Theben Smart Energy GmbH

[7] Evaluation Technical Report, Version 2, 2025-01-29, ETR Summary – CONEXA 1.6, TÜV Informationstechnik GmbH, (confidential document)

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

[9] Configuration list for the TOE HW, ALC_CMS.4 Konfigurationsliste Smart Meter Gateway CONEXA 3.0, Version 1.1, Theben Smart Energy GmbH (confidential document)

[10] Configuration list for the TOE SW, “ASSURANCE LIFE CYCLE – CONFIGURATION MANAGEMENT” DER CONEXA 3.0 (ALC_CMS.4), Version 3.85.0-cc, Theben Smart Energy GmbH (confidential document)

[11] Handbuch CONEXA 3.0 für Gateway Administrator, Version 2.13.3, 2024-11-25, Theben Smart Energy GmbH

[12] Handbuch CONEXA 3.0 für den Service-Techniker, Version 2.14.2, 2024-11-25, Theben Smart Energy GmbH

[13] Handbuch CONEXA 3.0 für den Letztverbraucher, 2.12.1, 2024-11-06, Theben Smart Energy GmbH

[14] Profilbeschreibungen CONEXA 3.0 Smart Meter Gateway, Version 2.16, 2024-08-02, Theben Smart Energy GmbH

[7] specifically

- 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 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 48, Version 1.0, Anforderungen an die Prüfung von Sicherheitsetiketten

[15] Logbucheinträge CONEXA 3.0 – Smart Meter Gateway, Version 1.11.0, 2024-08-07, Theben Smart Energy GmbH

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

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

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

[19] Anhang sichere Auslieferung, Version 0.16, 2024-11-29, Theben Smart Energy GmbH

[20] Impact Analysis Report – Smart Meter Gateway CONEXA, Version 3.01.1, 2025-01-20, Theben Smart Energy GmbH (confidential document)

[21] 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

[22] TR-03109:

Technische Richtlinie BSI TR-03109-1, Anlage IV, Feinspezifikation „Drahtlose LMN-Schnittstelle“, Teil a: „OMS Specification Volume 2, 13.12.2024, Primary Communication“, Version 2.0, German Federal Office for Information Security

Technische Richtlinie BSI TR-03109-1, Anlage IV, Feinspezifikation „Drahtgebundene LMN-Schnittstelle“, Teil a: „HDLC für LMN“, Version 2.0, 13.12.2024 , German Federal Office for Information Security

Technische Richtlinie BSI TR-03109-1, Anlage IV, Feinspezifikation „Drahtgebundene LMN-Schnittstelle“, Teil b: „SML-Smart Message Language“, Version 2.0, 13.12.2024, German Federal Office for Information Security

TR-03109-3: Technische Richtlinie BSI-TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, BSI, Version 1.1, 2014, Federal Office for Information Security

[23] TR-02102

Technische Richtlinie TR-02102 “Kryptographische Verfahren: Empfehlungen und Schlüssellängen”:

Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2024-01, Bundesamt für Sicherheit in der Informationstechnik.

Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2024-01, Bundesamt für Sicherheit in der Informationstechnik.

Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2024-02, Bundesamt für Sicherheit in der Informationstechnik.

[24] TR-03116-3: Technische Richtlinie 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.

[25] Standard of Implementation

BSI TR-03111: Elliptic Curve Cryptography (ECC). Version 2.10, German Federal Office for Information Security, 01.06.2018

[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), 2001-11-2, NIST, 2001.

[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. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report