Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0919-2019

for

CASA 1.0

from

EMH metering GmbH & Co. KG

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-0919-2019 (*)

Smart Meter Gateway

CASA 1.0

Software Version: 30000000__X026b
Hardware Version: 10 301 / 10 302 / 10 303 / 10 304

from EMH metering GmbH & Co. KG

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 AVA_VAN.5 and ALC_FLR.2

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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 as listed in the Certification Report 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, 17 December 2019

For the Federal Office for Information Security

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

Thomas Gast L.S.
Head of Branch

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG 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]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- 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

[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] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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]

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.

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ 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 CASA 1.0 has undergone the certification procedure at BSI.

The evaluation of the product CASA 1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 December 2019. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: EMH metering GmbH & Co. KG.

The product was developed by: EMH metering GmbH & Co. KG.

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. Considering the specific legal circumstances this certificate will have a validity of 8 years combined with a regular mandatory re-assessment after every 2 years. The certificate issued on 17 December 2019 is valid until 16 December 2027. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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 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 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,
5. to make sure that over the complete lifetime of the certificate a security module with a valid CC certificate is used.

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 CASA 1.0 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] EMH metering GmbH & Co. KG
Neu-Galliner Weg 1
19258 Gallin

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) is a communication unit used within an intelligent metering system represented by the product CASA except for the integrated Security Module and external communication interfaces. Besides the data processing, the Smart Meter Gateway offers the possibility to generate tariff rates, in order to enable network operators and consumers to control energy consumption in an intelligent way. As personal consumption data will be recorded, processed and transmitted in the Gateway, high demands are made on data protection and data security. The main functionality of the Gateway is the reception, the verification and the storage of measured values and status of the connected meters as well as the processing and the transfer of these measurements and status values. The transmission is done via the remote connection to authorized external entities, as for example, the metering point operators.

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 AVA_VAN.5 and ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. 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 Functions:

TOE Security Functionality	Addressed issue
SF.AU Audit	The TOE maintains three kinds of logs: • System Log • Consumer Log • Calibration Log All audit messages/entries contain information about the accountable user or event and further contain the following information: domain (log name), date, time, event type, level, subject identity, operation result, causing component and description. Furthermore, the consumer log contains all entries that are required for a billing verification, the system log includes all system relevant events and the calibration log persists of all information that is relevant for calibration purposes.
SF.CR Cryptography	The TOE implements the cryptographic functionality as required by [14], [TR 3109]. As defined by [8], this functionality covers the symmetric parts of the required cryptographic primitives. Furthermore, all ephemeral cryptographic keys used for TLS or symmetric AES encryption are destroyed using the method "zeroization" in accordance to [14], [FIPS 140-2] and the TOE will use the Security Module ([13]) to generate all necessary random numbers.
SF.UD User Data Protection	The TOE provides functionality to logically remove unused information by zeroization. All objects within the used databases are integrity protected. Furthermore, access control and multiple policies (gateway, firewall and

TOE Security Functionality	Addressed issue
	meter) protect the corresponding data by fixed defined rule-sets.
SF.IA Identification & Authentication	The TOE authenticates every user and external entity before allowing any other action on behalf of that user. User identities have the following security attributes: identity, status of identity, connecting network, role membership. The Gateway administrator can configure consumers with a username/password combination based identification & authentication or with a certificate based identification & authentication. The Gateway administrator can configure service technicians only with a certificate based identification & authentication. The identification & authentication of the Gateway administrator is implemented as certification-based, bidirectional mechanisms according to [14], [TR 3109-1].
SF.SM Security Management	The TOE includes functionality that allows its administration and configuration as well as updating the TOE's software. This functionality is only provided for the authenticated Gateway administrator. The following operations can be performed by the successfully authenticated Gateway administrator: • 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 and • Audit Log configuration.
SF.PR Privacy	The TOE provides mechanisms for communication concealing. A pseudonymization would only be used for processed Meter Data. The communication to external entities is performed over packet oriented networks. To conceal the communication, the packet size is mutable, also the transmitted content is padded to random size.
SF.SP Self-protection	The TOE provides a set of self-protection mechanisms that, in particular, comprise the self-test of the TOE, detection of replay attacks and the failure with preservation of a secure state.

Table 1: TOE Security Functions

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], chapters 3.3, 3.4 and 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:

CASA 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	CASA 1.0	10 301 / 10 302 / 10 303 / 10 304[7]	Secure Delivery Procedure via transport service and installation by a service technician or personal hand over
2	SW	SMGW Software	30000000__X026b	Pre-Installed on the HW
3	DOC	CASA 1.0 – Benutzerhandbuch für Letztverbraucher	Version: 1.17 SHA-256-Prüfsumme: 301e6f5a8553e7e0e531e7463020bcb119b6706fecc0a4019eb6ee2c542e0fce	Document can be requested from the developer
4	DOC	CASA 1.0 – Installations- und Konfigurationshandbuch für Service-Techniker und Gateway-Administratoren	Version: 1.17 SHA-256-Prüfsumme: 877ff4a38bb59828285d3a07523641c0f103091e8eb900b608d40630ab16a502	Document can be requested from the developer
5	DATA	CASA 1.0 – SMGW-Schnittstellenbeschreibung (CASA API)	Version: 1.24 SHA-256-Prüfsumme: a042a1bc3980f3230f11059930226e7096377e3bcdcbe34437ac9020b20cab4b	Document can be requested from the developer

Table 2: Deliverables of the TOE

The TOE itself consists of the hardware, firmware and software parts of the Smart Meter Gateway accompanied by the different guidance documents. For the physical parts (Hardware parts) two different delivery ways exist. In the first delivery variant the TOE is delivered within a special and secure safebag by a standard transportation service. A certified NFC-Tag (Cert.-ID: CC-19-175197) is welded in the right side foil of the safebag. The safebag possesses also security features to prevent manipulations with cutting, welding and chemical solvents. Furthermore, the freight hold needs to be sealed. Each seal possesses a unique seal number, which belongs to the tracking information of the delivery. The TOE is packed into the safebag at the end of the production chain in the

[7] Please note that this is a set of four alternative TOE Hardware Versions, denoted by the forward slash separator '/'; each variant describes the application of specific equivalent hardware components.

secure production environment. Tracking information for the secure delivery is stored into the NFC-Tag. Before the receiver opens the safebag, they have to verify the integrity of the safebag and the integrity and authenticity of the tracking information stored within the NFC-Tag. After a successful verification, the TOE can be installed at the consumer site by a service technician.

In the second variant the TOE can be directly delivered by two employees of the developer without safebag. In this case, only a maximum of 10 TOEs can be transported and the transport time is limited to 24 hours. Continual monitoring of the TOE by the carrier during the transport is necessary.

Parallel to the delivery procedures, all places where the TOE 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 TOE 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 firmware and software are pre-installed on the hardware and therefore part of the physical delivery. All users can uniquely identify it by connecting to the TOE and using the commands described in the relevant guidance document.

The guidance documents can be requested from the developer (standard delivery). After the standard delivery, they can be uniquely identified by checking the hash value which is also included in the Security Target and the Certification Report (which both 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.

Specific details concerning the above mentioned security policies can be found in chapter 7 of the Security Target [6].

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 shall 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,
  - Random Number Generation.

  The Security Module used shall be certified according to [13] 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 the Security Target [6] 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 a 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,
  - if devices in the HAN have a separate connection to parties in the WAN (beside 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 [TR 03109-3]. It shall also be ensured that the keys are brought into the Gateway in a secure way by the Gateway Administrator.

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

5. Architectural Information

The evaluator has determined that the following subsystems of the TOE are identified as follows:

- Cryptography: Contains all functionalities to realize security functionalities with the Hardware Security Module (SM).
- System Audit: Logs all important activities of the TOE. For potential discrepancies the GWA will be informed.
- Networking: Implements the TSFIs IF_GW_WAN, IF_GW_CLS and IF_GW_SRV.
- Metering: Responsible for the collection, storage and transport of the meter data.

- System Time: Manages the system time and time synchronization.
- Boot: Responsible for the secure boot of the TOE.
- Operating System: Provides the basis for running applications. It manages the system resources of main memory, non-volatile memory and connected interface blocks.
- Hardware: Includes the SMGW hardware: circuit boards, active and passive components including enclosures.

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

7.1. Developer Tests

Test configuration: All developer tests in the context of the evaluation have been conducted using multiple TOE samples in two different configurations (final and SSH), both in IPv4 version. Hereby, final configuration corresponds to the final unmodified TOE version (SW version 30000000__X026b and HW version 10 301), the SSH configuration is based on the same TOE version, but was slightly modified to enable detailed testing where this kind of additional access was necessary.

The developer’s testing approach was to systematically test the TOE separated into four different subsets. One for each major interface group (WAN, HAN and LMN) and one for manual testing of meters or LEDs. Hence, the following test groups are identified within the documentation: LMN test environment, WAN test environment, HAN test environment, and manual hardware tests.

Based on this subdivision, the full behaviour of the TSF was tested by developing corresponding test cases during the development of the TOE. The corresponding coverage and depth in testing for all SFRs, TSFIs as well as the TOE behaviour on the level of subsystems were also summarized by the developer and evaluated by the evaluation body without relevant deviations. The overall test amount is about 650 test cases.

The evaluator checked the actual test results of the developer’s test for inconsistencies with the expected test results. No inconsistencies have been found.

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.

7.2. Independent Tests

Test configuration: 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 and used a modified TOE for side-channel analysis (EMA) and testing of the case seal.

The evaluator tested all TSFI, except IF_GW_CLS. Hereby, IF_GW_CLS is secured with the same major mechanisms as the other HAN interfaces, but more complicated to trigger. Hence, the evaluation facility decided to test only the other HAN interfaces and use source code analyses to verify that IF_GW_CLS uses the same security mechanisms as defined within the ST [6].

Independent and penetration tests of the evaluation body are mainly performed on a stand-alone test-solution, containing approx. 1000 automated tests developed by TÜViT, partitioned according to the SF established in [6], chapter 7. Using this environment, every necessary role with corresponding rights (GWA, service technician, meters and consumers, might be emulated at the appropriate interface. In particular, for testing IF_GW_MTR, it contains a “meter simulator”, which allows to emulate and connect multiple meters, controlling their behaviour (e.g. for inducing errors). Using the dedicated crypto proxy, it is further possible to extract the nested CMS data, supported by the enhanced Wireshark, which was enriched by the implementation of various dissectors. Those test cases were supplemented by additional manual tests using the developer resources and further manual penetration tests on the HAN interface.

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

7.3. Penetration Tests

Test configuration: The TOE was delivered by the developer in different variants. Beside the final operational variant, including mobile communication (LTE or GPRS), a final operational variant prepared for side-channel analyses, a special ATE variant with extended test possibilities and SSH interface to directly access the TOE and view/modify data such as time-stamps, and a TOE case without interiority for case and sealing tests have been delivered. These variants enable tests that would not be possible on the release TOE due to applied security mechanisms.

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, 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.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

TOE reference	TOE configuration
TOE Identification	CASA 1.0
Software Version Number	30000000__X026b
Hardware Version Number	10 301 / 10 302 / 10 303 / 10 304[8]

Table 3: TOE configuration

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 34, 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 AVA_VAN.5 and ALC_FLR.2 augmented for this TOE evaluation.

  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 AVA_VAN.5 and ALC_FLR.2

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.

[8] Please note that this is a set of four alternative TOE Hardware Versions, denoted by the forward slash separator '/'; each variant describes the application of specific equivalent hardware components.

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_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE: [RFC5289] ECDSA: [TR 03111] AES: [FIPS 197] HMAC: [RFC 2104] brainpoolPxxxr1: [RFC 5639] secpxxxr1: [SECG-SEC2] CBC: [NIST SP800-38A] GCM: [NIST SP800-38D] SHA: [FIPS 180-4]	AES: 128bit, 256bit EC: secp256r1, secp384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	[TR03109]	2025+
Key generation for CMS containers	key generation algorithms: ecka-eg-X963KDF-SHA256, ecka-eg-X963KDF-SHA384, ecka-eg-X963KDF-SHA512 combined with key wrap algorithms: id-aes128-wrap, id-aes192-wrap, id-aes256-wrap	key generation: [TR 03111], key wrap: [RFC 3394]	128bit, 192bit, 256bit	[TR03109]	2025+
Encryption / decryption /integrity of CMS container	id-aes128-GCM id-aes192-GCM id-aes256-GCM id-aes-CBC-CMAC-128 id-aes-CBC-CMAC-192 id-aes-CBC-CMAC-256	id-aesxxx-gcm: [RFC 5084], id-aes-CBC-CMAC-xxx: [TR 03109-1-I], AES: [FIPS 197], GCM: [NIST SP800-38D], CBC: [NIST SP800-38A], CMAC: [NIST SP800-38B]	128bit, 192bit, 256bit	[TR03109]	2025+
Key generation	AES-CMAC	AES-CMAC: [RFC	128bit	[TR03109]	2025+

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
for meter data		4493], AES: [FIPS 197], CMAC: [NIST SP800-38B]			
Encryption/ decryption, integrity of meter data	AES-CBC AES-CMAC	AES: [FIPS 197], CBC: [NIST SP800-38A], AES-CMAC: [RFC 4493], CMAC: [NIST SP800-38B]	128bit	[TR03109]	2025+
Basic support of integrity, authenticity	SHA-256, SHA-384, SHA-512	[FIPS180-4]	-	[TR03109]	2025+
Encryption / decryption, integrity of TSFI	XTS-AES	[IEEE P1619]	128bit	[TR03109]	2025+
Remarks	Integrity of firmware updates and stored binaries of TSFI are not defined in SFRs per ST [6], but they are implemented as ARC mechanisms.				

Table 4: 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).

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

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
CMS	Cryptographic Message Syntax
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FLR	Flaw Remediation
GWA	Gateway Administrator
HAN	Home Area Network
HTTP	Hypertext Transfer Protocol
HW	Hardware
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interfaces

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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012
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[9]
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-0919-2019, Version 2.00, 2019-12-16, CASA 1.0 Security Target, EMH metering GmbH & Co. KG

[7] Evaluation Technical Report, Version 1, 2019-12-16, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), 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

CASA-Konfigurationsliste, Version 9, 2019-12-16, Konfigurationsliste (confidential document)

[10] CASA (CASA-AGD) Benutzerhandbuch für Letztverbraucher (LV), Version 1.17, 2019-12-16

[11] CASA (CASA-AGD) Installations- und Konfigurationshandbuch für Service-Techniker und Gateway-Administratoren, Version 1.17, 2019-12-16

[9] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- 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, 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

[12] CASA 1.0 SMGW-Schnittstellenbeschreibung, Version 1.24, 2019-11-29

[13] Protection Profile for the Security Module of a Smart Meter Gateway (BSI-CC-PP-0077-V2). Version 1.03. BSI, 11.12.2014

[14] Standard of Application

[TR 03109] BSI TR-03109. Version 1.0.1. BSI, 11.11.2015

[TR 03109-1] BSI TR-03109-1,Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0, 18.03.2013

[TR 03109-3] BSI TR-03109-3, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, BSI, Version 1.1, 2014

[TR 03111] BSI TR-03111: Elliptic Curve Cryptography (ECC). Version 2.10. BSI, 01.06.2018

[TR 03116] BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme. BSI, 04.04.2016

[FIPS 140-2] NIST FIPS PUB 140-2: Security Requirements for Cryptographic Modules, Part 2. NIST, 2001

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

[FIPS 197] NIST FIPS PUB 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES). 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 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.

[IEEE P1619] IEEE P1619™/D16 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. IEEE, May 2007.

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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