Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0822-V2-2020

for

SMARTY IQ-LTE, Version 1.0

from

Sagemcom Dr. Neuhaus 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-0822-V2-2020 (*)

Smart Meter Gateway

SMARTY IQ-LTE, Version 1.0
Hardware Version: DNT8209/3.3
Software Version: 2.0.2972
Operating System Version: DNT8209-21

from	Sagemcom Dr. Neuhaus 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 AVA_VAN.5 and ALC_FLR.2

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 configurations 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, 27 November 2020

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

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 (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.
- 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 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+ 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 SMARTY IQ-LTE, Version 1.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0822-2019. Specific results from the evaluation process BSI-DSZ-CC-0822-2019 were re-used.

The evaluation of the product SMARTY IQ-LTE, Version 1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 25 November 2020. 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:
Sagemcom Dr. Neuhaus GmbH.

The product was developed by: Sagemcom Dr. Neuhaus 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. Considering the specific legal circumstances this certificate issued on 27 November 2020 is valid until 24 September 2027 provided that a regular mandatory re-assessment after every 2 years will be succeeded. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

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 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 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 SMARTY IQ-LTE, Version 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] Sagemcom Dr. Neuhaus GmbH
Papenreye 65
22453 Hamburg
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), the SMARTY IQ-LTE, Version 1.0, is an electronic unit comprising hardware, software and firmware. It serves as a Gateway in a complex Smart Metering Infrastructure, which is used for collection, storage and provision of meter data from one or more meters of one or multiple commodities to potentially multiple external entities. A complete system for smart metering comprises different functional units, whereby only the Smart Meter Gateway functionality is in the focus of the evaluated TOE.

The hardware device also contains a certified security module (product name “TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE”, BSI-DSZ-CC-0957-V2-2016), which is not part of the TOE, but used by the TOE for specific cryptographic services.

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 Functionality:

TOE Security Functionality	Addressed issue
SF.CR, Cryptographic Support	The TOE implements the cryptographic functionality as required by [17], [TR-3109]. As defined by [8] this functionality covers the symmetric parts of the required cryptographic primitives. The TOE utilizes the services of the security module [16] for all asymmetric cryptographic primitives. The TOE encrypts all TSF and user data if they are not in use. The TOE will use the Security Module to generate all necessary random numbers.
SF.IA, Identification and 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, blocking flag, login and logout time. 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 mechanism according [17], [TR-03109].
SF.PR, Privacy	The TOE provides mechanisms for communication concealing. 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.AU, Security Audit	The TOE implements three different audit logs:

TOE Security Functionality	Addressed issue
	a) System Log, b) Consumer Log, and c) Calibration Log. All audit messages/entries contain information about the accountable user or event and they further contain the following information: domain (log name), date, time, event type, level, subject identity, operation result, causing component, 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.SM, Security Management	The TOE only provides authorized users with security management functions. Hereby, all authorized users have the capability to trigger self-tests. Additionally, the consumer may also display the current version number of the TOE and the current time. Concerning management functionalities, the Service Technician may only change the parameters for the network access for WAN during the installation process and the Gateway Administrator may configure all aspects of the SMGW, which is exclusively possible via IF_GW_WAN. For documentation, see the corresponding HGP protocol [13].
SF.SP, Self-Protection	The TOE implements functionality for self-protection, for instance preserving a secure state in case of failures (for example integrity errors). If the system time is not valid, all recorded measurement data will marked for the EMT.
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 firewall policies protect the corresponding data.

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:

SMARTY IQ-LTE, Version 1.0

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Form of Delivery
1	HW	SMARTY IQ-LTE Version 1.0	Hardware Version: DNT8209/3.3	Standard Delivery via transport service and installation by a service technician or personal hand over.
2	SW	Operating System	DNT8209-21	Pre-Installed on the HW
3	SW	SMGW Application	2.0.2972	Pre-Installed on the HW
4	DOC	Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, [10]	1.25	Download from https secured website hash256 cf119cd4a4b128e2b41648ae73e2fa4eaa1a6bcb8e8911f6ce1387d2645ada95
5	DOC	Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, [11]	1.23	Download from https secured website hash256 bb29af033104746a7fd5baeb433d6f8010bdb12e13cbb2f1af060a4ba0a7a05a
6	DOC	Sichere Lieferkette, [12]	1.3	Download from https secured website hash256 3ad99a0fa18b7918821ac70255a031d4b0d88c64ea57cd22402748be8b21b375
7	DOC	Anlage zum AGD: - Http Gateway Protocol 2.4, [13]	2.4.026	Download from https secured website hash256 7448a50402a3c47331429e932353575b72fedb2743e928dd2fc8eed1ef8c3049
8	DOC	Anlage zum AGD: Übersicht der Audit Records, [14]	1.36	Download from https secured website hash256 c4c2cf8dadd7950c3ee97e04b9f29372705dcbe3495a18c297f091953850a9df
9	DOC	Anlage zum AGD: Übersicht der versendeten Events, [15]	1.36	Download from https secured website hash256 1d02ebcaa59478385c346341f1b5a36d5e6399e274ca40845735852b30bc4f80

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 scenario SMGW are delivered within a special and secure transport box (pylocx Box) by a standard transportation service. The secure transport box can only be opened by authorized individuals by using a special key pad and a valid and individual 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. In the second scenario SMGW can be delivered without such secure boxes but the general requirements for the transport are increase. For example the freight hold needs to be sealed and the transport needs to be supervised by two drivers. Furthermore, the transport time is limited to 36 hours and overnight breaks are not allowed. If the SMGWs shall be stored without secure transport box, the store has to be certified against Common Criteria. 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 firmware and software is 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 downloaded by a https secured website (standard delivery). After they are downloaded they can be uniquely identified by checking the hash sum 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 the Security Target [6], chapter 7.

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 and Random Number Generation. The Security Module used shall be certified according to [16] 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 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 the TR-03109 [17]. 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 following subsystems and modules of the TOE are identified as follows (including a short description of the corresponding objective extracted from):

- cryptmgr: Contains all functionalities to realize security functionalities with the Hardware Security Module.
- dataproc: Persists all configuration profiles and other settings in an encrypted database.
- hanmgr: Contains all functionalities to set up encrypted connections in the LAN.
- hardware: Includes the SMGW hardware: circuit boards, active and passive components including enclosures.
- lmn485: Contains all functionalities to use the LMN network.
- lmnmgr: Contains all functionalities to capture and process metrics.
- lmnwmbus: Contains all functionalities to use the wireless LMN network.
- logctrl: Accepts the audit records generated in the other subsystem and stores them accordingly in System, Calibration log and Consumer log required by TR.
- middleware: Contains general functionalities that are provided to other subsystems.
- miscmgr: Miscmgr is a summary of necessary functionalities, which are not related to the meter data acquisition.
- netmgr: Contains all functionalities to manage the physical network interfaces in the LAN and WAN.
- OS: Provides the basis for running applications. It manages the system resources of main memory, non-volatile memory and connected interface blocks.
- wanmgr: Contains all functionalities to set up and manage encrypted connections to the Gateway Administrator and the External Market Participant.

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

For this re-certification the test results from the basic evaluation were reused. The description of the test activities is repeated here for better readability.

7.1. Test configuration

The TOE in the evaluated configuration has been tested (cmp. chapter 8).

Only where necessary to enable detailed testing, slightly modified TOE configurations (e.g. a TOE with SSH capabilities) were used, demonstrably without influencing the tested security functionality.

7.2. Developer tests

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 coverage and depth in testing all SFs, TSFIs as well as the TOE behaviour and existing interactions on level of subsystems were also summarized by the developer and evaluated by the evaluation body without relevant deviations in the developer test documentation.

The main testing tool is a proprietary test tool (WANSIM) developed and provided by the developer. With it, all tests can be executed.

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.

7.3. Independent tests

The evaluation body used the same TOE variants, test configurations and test environment as the developer during functional testing. Additionally the evaluation body used an independent test system (Exceeding Solutions) to perform the independent tests of the ITSEF and used additional modification of the TOE for side channel analysis (EMA) and testing of the case seal.

All TSFI have been tested by the evaluator, 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.

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

7.4. Penetration tests

The evaluation body conducted penetration testing based on functional areas of concern derived from SFRs and architectural mechanisms.

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; moreover, no attack scenario with the attack potential High was actually successful.

The TOE passed all developer and evaluation body tests.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

SMARTY IQ-LTE, Version 1.0
Hardware Version: DNT8209/3.3
Software Version: 2.0.2972
Operating System Version: DNT8209-21

The certified version of the TOE is built into the case of the Smart Meter Gateway and can be identified by the laser engraving showing the hardware information as described in the following example “DNT8209/3.3”.

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] (AIS34) and guidance specific for the technology of the product [4] (AIS 34, 46, 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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0822-2019, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the update of the vulnerability assessment. As a result of the updated vulnerability assessment the GPRS configuration was removed from the certified scope, so that only the LTE configuration remains certified.

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.

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
Basic support of integrity, authenticity	SHA-256, SHA-384	[FIPS180-4]	Hash length = 256, 384	TR-03109 [17]	2026+
Encryption / decryption, integrity of TSFI	AES-GCM	[FIPS-197], [SP800-38D]	256	TR-03116 [17]	2026+
Key generation for CMS containers	ECKA-EG	[RFC5652], [RFC5639], [RFC6161], [X9.62] [FIPS 186-4]	128, 192 and 256	TR-03111 [17]	2026+
Encryption / decryption /integrity of CMS container	AES-CBC-CMAC	[RFC5652], [RFC6033] [FIPS-197], [RFC4493], [SP800-38A]	128, 192 and 256	TR-03109 [17]	2026+
Encryption / decryption / integrity of CMS container	AES-GCM	[RFC5652], [RFC5084], [FIPS-197] [SP800-38D]	128, 192 and 256	TR-03109 [17]	2026+
Key generation for meter data	AES-CMAC	[RFC4493] [FIPS-197]	128, 256	TR-03109 [17]	2026+
Encryption/ decryption, integrity of meter data	AES-CBC	[RFC4493] [FIPS-197] [SP800-38A]	128	TR-03109 [17]	2026+
TLS key establishment	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	[RFC5246], [RFC8422], [RFC5639], [FIPS-180-4], [FIPS-186-4], [RFC 2104]	256, 384	TR-03109 [17]	2026+
TLS 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	[RFC5246], [RFC6090], [RFC5639], [FIPS-186-4], [FIPS-197].	256, 384	TR-03109 [17]	2026+
TLS record layer encryption	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,	[RFC5246], [FIPS-197], [SP800-38A]	AES-CBC: 128, 256	TR-03109 [17]	2026+

	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384				
TLS record layer encryption and integrity	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	[RFC5246], [FIPS-197], [RFC5288], [SP800-38D]	AES-GCM: 128, 256	TR-03109 [17]	2026+
TLS record integrity	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	[RFC5246], [FIPS180-4], [RFC2104], [RFC5289].	HMAC-SHA: 256, 384	TR-03109 [17]	2026+
Integrity of configuration data	CMAC	[SP-800-38B], [RFC4493].	128	TR-02102-2 [17]	2026+
Integrity of firmware updates	ECDSA	[X9.62], [RFC6090], [RFC5639].	256	TR-02102-2 [17]	2026+
Integrity of TSFI	ECDSA	[X9.62], [RFC6090], [RFC5639]	256	TR-02102-2 [17]	2026+

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).

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FLR	Flaw remediation
HAN	Home Area Network
HGP	HTTP Gateway Protocol
HTTP	Hypertext Transfer Protocol
HW	Hardware
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LMN	Local Metrological Network
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMGW	Smart Meter Gateway
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interfaces
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 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[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-0822-V2-2020, Version 1.29, 2020-10-30, SMARTY IQ-GPRS / LTE Security Target, Sagemcom Dr. Neuhaus GmbH

[7] Evaluation Technical Report, Version 5, 2020-11-20, 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 (confidential documents)

filelist_OS_TFS, 2018-07-09

filelist_sln8209, 2019-10-16

8209SE011_SMGw_CPU_USB.xls, Version 3.3, 2018-09-11

8209SE030_SMGw_Basis_LTE.xls, Version 1.3, 2018-09-26

SMGW_2_Source_Bauteile.xlsx

[7] 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

Documentation according to:

Lebenszyklusunterstützung, chap. 8.4.2 Dokumentation, Version 1.20, 2019-09-18

[10] Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, Version 1.25, 2019-07-18

[11] Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, Version 1.23, 2019-09-16

[12] Sichere Lieferkette, Version 1.3, 2019-09-13

[13] Anlage zum AGD: - Http Gateway Protocol 2.4, Version 2.4.026, 2019-01-22

[14] Anlage zum AGD: Übersicht der Audit Records, Version 1.36, 2019-05-24

[15] Anlage zum AGD: Übersicht der versendeten Events, Version 1.36, 2019-05-24

[16] Common Criteria Protection Profile for a Security Module for Smart Metering Systems (BSI-CC-PP-0077-V2-2015), Version 1.03, 11.12.2014, Version Bundesamt für Sicherheit in der Informationstechnik.

[17] Standard of Application

[TR-02102-2], Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2015-01, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109], Technische Richtlinie BSI TR-03109, Version 1.0, 18.03.2013, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03111], BSI - Technical Guideline, Elliptic Curve Cryptography, Version 2.0, 2012-06-28, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03116], Technische Richtlinie BSI TR-03116Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, Stand 2019, 2019-01-11

[RFC8422], ETF: Y. Nir, J. Josefsson, M. Pegourie-Gonnard: RFC 8422, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier, August 2018

[RFC6161], Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type, April 2011

[RFC6090], Fundamental Elliptic Curve Cryptography Algorithm, February 2011

[RFC6033], Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type, December 2010

[RFC5652], RFC 5652 - Cryptographic Message Syntax (CMS), IETF Trust and the persons identified as the document authors, September 2009 (http://tools.ietf.org/html/rfc5652).

[RFC5639], RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010 (http://www.ietf.org/rfc/rfc5639.txt).

[RFC5289], RFC 8289 - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (CGM), M. Rescorla, August 2008 (https://tools.ietf.org/html/rfc5289).

[RFC5288], AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008

[RFC5246], RFC 5246 - The Transport Layer Security (TLS) Protocol, Version 1.2, Dierks & Rescorla - Standard Track, August 2008 (http://www.ietf.org/rfc/rfc5246.txt).

[RFC5084], RFC5289 - Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), R. Housley, November 2007 (https://tools.ietf.org/html/rfc5084).

[RFC4493], RFC4493 - The AES-CMAC Algorithm, JH. Song, R. Poovendran, J. Lee, T. Iwata, June 2006 (https://tools.ietf.org/html/rfc4493).

[RFC2104], Minimal Encapsulation within IP, October 1996

[FIPS180-4], FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.

[FIPS-186-4], Federal Information Processing Standards Publication FIPS PUB 186 4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST)

[FIPS-197], Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001

[X9.62], American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute.

[SP800-38A], NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

[SP800-38B], NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST).

[SP800-38D], NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007, National Institute of Standards and Technology (NIST).

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 detailed 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