

Certification Report

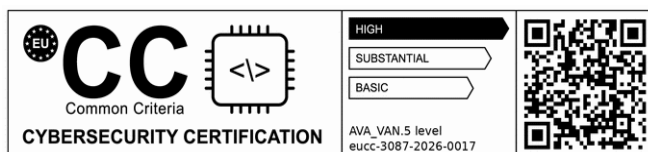
EUCC-3087-2026-0017
Administration ID
BSI-DSZ-CC-0822-V8-2026

for

SMARTY IQ-LTE, Version 1.5

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 9582-11

Contents

A. Certification.....	4
1. Preliminary Remarks.....	4
2. Specifications of the Certification Procedure.....	4
3. Recognition Agreements.....	5
4. Performance of Evaluation and Certification.....	5
5. Publication.....	7
B. Certification Results.....	8
1. Executive Summary.....	9
2. Identification of the TOE.....	9
3. Security Policy.....	11
4. Assumptions and Clarification of Scope.....	12
5. Architectural Information.....	14
6. Supplementary Cybersecurity Information.....	14
7. IT Product Testing.....	15
8. Evaluated Configuration.....	15
9. Results of the Evaluation.....	16
10. Obligations and Notes for the Usage of the TOE.....	19
11. Security Target.....	19
12. Regulation specific aspects (eIDAS, QES).....	19
13. Definitions.....	19
14. Bibliography.....	22
C. Annexes.....	26

A. Certification

1. Preliminary Remarks

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

By implementing the Cybersecurity Act¹, certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG² Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security²

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

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

- BSI Certification and Approval Ordinance³
- BMI Regulations on Ex-parte Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 Common Criteria for IT Security Evaluation (CC), Version 3.1 R5 [CC]
- ISO/IEC 18045 Common Methodology for IT Security Evaluation (CEM), Version 3.1 R5 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Recognition Agreements

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

3.1. International Recognition of CC – Certificates (CCRA)

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

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

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

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

4. Performance of Evaluation and Certification

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

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

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

- The TOE SMARTY IQ-LTE, Version 1.5 has been re-certified by the certification body of the Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-0822-V7-2025. Specific results from the evaluation process were re-used.
- The evaluation of the product SMARTY IQ-LTE, Version 1.5 was carried out by TÜV Informationstechnik GmbH, located at Unternehmensgruppe TÜV NORD, Am TÜV 1, 45307 Essen.
- The evaluation was completed on 21 September 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: Sagemcom Dr. Neuhaus GmbH.
- The assessed TOE was developed by: Sagemcom Dr. Neuhaus GmbH.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

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

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

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

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

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product's resistance, the maximum validity period of the certificate is limited. The certificate issued on 28 September 2026 is valid until 27 September 2036 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

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

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the

holder of the certificate applies for measures under EUCC scheme's assurance continuity (i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE SMARTY IQ-LTE, Version 1.5 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate⁵ has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁵ Sagemcom Dr. Neuhaus GmbH
Papenreye 65
22453 Hamburg
Deutschland

B. Certification Results

The following chapters summarise the assessment results of the

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

1. Executive Summary

The Target of Evaluation (TOE) SMARTY IQ-LTE, Version 1.5 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 product SMARTY IQ-LTE, Version 1.5 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a re-certification based on administration ID BSI-DSZ-CC-0822-V7-2025. Specific results from the evaluation process BSI-DSZ-CC-0822-V7-2025 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product SMARTY IQ-LTE, Version 1.5 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 21 September 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).

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

The evaluation has confirmed:

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

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

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

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

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

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

2. Identification of the TOE

The information and communications technology product is identified as follows:

SMARTY IQ-LTE, Version 1.5

Holder of the certificate: Sagemcom Dr. Neuhaus GmbH
Papenreye 65
22453 Hamburg
Deutschland
<https://www.sagemcom.com/smgw>

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SMARTY IQ-LTE Version 1.5	DNT8209/3.3/A DNT8209/3.3/B DNT8209/4.0/B DNT8209/4.5/B	Secure delivery process as described below this table
2	SW	Operating System	DNT8233-06	Pre-Installed on the HW
3	SW	SMGW Application	2.1.6016	Pre-Installed on the HW
4	DOC	Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, [AGD_OPE]	1.202	Download from https secured website Hash SHA256: 9e40900bf6434d2edffbd31522188fb3c26844522db60570064989b6faff803b
5	DOC	Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, [AGD_PRE]	1.203	Download from https secured website Hash SHA256: 9fbcf4c0fc6e97867a77f5741490e4bbe1e68a0e9c67888c0d45d5f02a7dd2c2
6	DOC	Sichere Lieferkette, [ALC_SichereLieferkette]	1.200	Download from https secured website Hash SHA256: e37beb96a26fb15f9f82aed4ebc91a2bd3fcccceca1ac75c2335a0fa847f89e48
7	DOC	Anlage zum AGD: HGP 2.5 SMGW - Http Gateway Protocol [AGD_HGP]	2.5.215	Download from https secured website Hash SHA256: 0059153aab576a783f7989989e04afb7d5077d61d3a2514dad78853cae093c0f
8	DOC	Anlage zum AGD: Übersicht der Audit Records, [AGD_Audit]	1.205	Download from https secured website Hash SHA256: b6c373ce2eea20794c1c31a846d8ba63610b9abfcb286fcc48b53204a30f43ca
9	DOC	Anlage zum AGD: Übersicht der versendeten Events, [AGD_Events]	1.205	Download from https secured website Hash SHA256: 35d9bba42c1ba1fef90ff05c969178b5a4d884c546c0b649145d7b43cd278a4e

Table 1: Deliverables of the TOE

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

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) three 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. 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 third scenario describes the MSB supply chain defined by the Federal Office for Information Security (BSI) [MSB-LK]. In this case, the MSB's responsibility for the secure supply chain begins immediately upon receipt of goods from the initial delivery. If ownership of the SMGW is transferred to another MSB, the responsibility for the secure MSB supply chain is transferred accordingly.

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.

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 (ST).

A reference and description of the vulnerability handling policy and the assurance continuity policy can be found in [VulHand].

4. Assumptions and Clarification of Scope

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

Assumptions on the TOE's usage and deployment:

- A.ExternalPrivacy: It is assumed that authorised and authenticated external entities receiving any kind of privacy-relevant data or billing-relevant data and the applications that they operate are trustworthy (in the context of the data that they receive) and do not perform unauthorised analyses of this data with respect to the corresponding consumer(s).
- A.TrustedAdmins: It is assumed that the Gateway Administrator and the Service Technician are trustworthy and well-trained.
- A.PhysicalProtection: It is assumed that the TOE is installed in a non-public environment within the premises of the consumer which provides a basic level of physical protection. This protection covers the TOE, the Meter(s) that the TOE communicates with and the communication channel between the TOE and its Security Module.
- A.ProcessProfile: The Processing Profiles that are used when handling data are assumed to be trustworthy and correct.
- A.Update: It is assumed that firmware updates for the Gateway that can be provided by an authorised external entity have undergone a certification process according to this Protection Profile before they are issued and can therefore be assumed to be correctly implemented. It is further assumed that the external entity that is authorised to provide the update is trustworthy and will not introduce any malware into a firmware update.
- A.Network: It is assumed 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.
- A.Keygen: It is assumed that the ECC key pair for a Meter (TLS) is generated securely according to the [TR-03109-3] and brought into the Gateway in a secure way by the Gateway Administrator.

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

List of objectives which have to be met by the the environment:

- 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 [SM-PP] and shall be used in accordance with its relevant guidance documentation.

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

- 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-03109-3]. 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 [ST].

5. Architectural Information

The TOE is decomposed into the following subsystems:

- cryptmgr: Contains all functionalities to realize the cryptographic security functionalities together with the non-TOE 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 subsystems and stores them in the System-, Calibration- and Consumer-log as required by [TR-03109].
- 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 the main memory, the non-volatile memory and the connected interface blocks.
- wanmgr: Contains all functionalities to set up and manage encrypted connections to the Gateway Administrator and the External Market Participant.

6. Supplementary Cybersecurity Information

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

Period during which support is offered: Security updates are provided by Sagemcom Dr. Neuhaus. Installation is carried out by the metering point operator's gateway administrator. Operators are promptly informed of available updates. The time frame for providing updates is stipulated in the contracts with metering point operators and, in all cases, meets the statutory minimum requirement of five years. An eight-year period is typically agreed upon.

Contact information of the manufacturer: Neuhaus.Support@sagemcom.com can be contacted to report security-related or functional vulnerabilities.

Known software issues are documented in the release notes. Where possible, workarounds are also provided there. The release notes are published alongside the documents for safe operation.

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

7. IT Product Testing

All tests have been carried out by ITSEF:

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Am TÜV 1

45307 Essen

under the responsibility of certification Body

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

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

The EUCC regulations were complemented by JIL guidelines and AIS scheme interpretations in case no equivalent EUCC regulation is available.

The evaluation was realised in accordance with [CC], while considering [CEM]. Interpretations of AIS 1, AIS 14, AIS 19, AIS 32, AIS 34, AIS 46 and AIS 48 [AIS] were considered.

The tests were executed on the evaluated TOE version (Software-Version 2.1.6016, OS Version DNT8233-06, HW version DNT8209/3.3/A) in the previous certification process with the administration ID BSI-DSZ-CC-0822-V7-2025. The test results are still valid for this certification process.

The developer's testing approach was to systematically test all the TSFI next to a deeper consideration of all TOE subsystems, internal interactions and concrete SFR tests.

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 and TSFI perform as specified. The evaluation body used an independent test system (Exceeding Solutions) to perform the independent tests of the ITSEF and used an additional modification of the TOE for testing of the case seal.

All TSFI have been tested by the evaluation body in the previous certification process with the administration ID BSI-DSZ-CC-0822-V7-2025:

The evaluation body chose to repeat a defined subset of the developer tests with the intent to cover the existing interfaces and the implemented security functionality.

Independent and penetration tests of the evaluation body are mainly performed on stand-alone test equipment, containing approx. 3000 automated test cases in about 150 test suites developed by TÜVIT, partitioned according to the security functions established in the Security Target [6], chapter 7. Using this environment, every necessary role (Gateway

Administrator, Service Technician, Consumer) with corresponding rights and meters might be emulated at the appropriate interface.

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

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 prioritised 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 test results remain valid and were extended by some specific testcases for SMGW certificate change processes.

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. The test results are still valid for this certification process.

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

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

SMARTY IQ-LTE, Version 1.5

Hardware Version: DNT8209/3.3/A, DNT8209/3.3/B, DNT8209/4.0/B, DNT8209/4.5/B

Software Version: 2.1.6016

Operating System Version: DNT8233-06

9. Results of the Evaluation

9.1. CC specific results

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

On advise by the Certification Body and consent by the certificate holder the following guidance further specific for the technology of the product [AIS] (AIS 34) was applied: AIS 46, AIS 48.

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

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

The certificate

- is uniquely identified by: EUCC-3087-2026-0017,
administration ID BSI-DSZ-CC-0822-V8-2026
- was issued on: 28 September 2026
- is valid until: 27 September 2036

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (<https://www.bsi.bund.de>).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Period of validity
1	Basic support of integrity, authenticity	SHA-256, SHA-384	[FIPS-180-4]	Hash length = 256, 384	TR-03109	2030+
2	Encryption / decryption, integrity of TSFI	AES-GCM	[FIPS-197] [SP800-38D]	256	TR-03116	2030+
3	Key generation for CMS containers	ECKA-EG	[RFC5652] [RFC5639] [RFC6161] [X9.62] [FIPS-186-4]	128, 192 and 256	TR-03111	2030+
4	Encryption / decryption / integrity of CMS container	AES-CBC-CMAC	[RFC5652] [RFC6033] [FIPS-197] [RFC4493] [SP800-38A]	128, 192 and 256	TR-03109	2030+
5	Encryption / decryption / integrity of CMS container	AES-GCM	[RFC5652] [RFC5084] [FIPS-197] [SP800-38D]	128, 192 and 256	TR-03109	2030+

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Period of validity
6	Key generation for meter data	AES-CMAC	[RFC4493] [FIPS-197]	128, 256	TR-03109	2030+
7	Encryption/decryption, integrity of meter data	AES-CBC	[RFC4493] [FIPS-197] [SP800-38A]	128	TR-03109	2030+
8	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] [RFC2104]	256, 384	TR-03109	2030+
9	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	2030+
10	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, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	[RFC5246] [FIPS-197] [SP800-38A]	AES-CBC: 128, 256	TR-03109	2030+

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Period of validity
11	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	2030+
12	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	2030+
13	Integrity of configuration data	CMAC	[SP-800-38B] [RFC4493]	128	TR-02102	2032+
14	Integrity of firmware updates	ECDSA	[X9.62] [RFC6090] [RFC5639]	256	TR-02102	2032+
15	Integrity of TSFI	ECDSA	[X9.62] [RFC6090] [RFC5639]	256	TR-02102	2032+

Table 2: TOE cryptographic functionality

According to [TR-03109], [TR-03111], [TR-03116] or [TR-02102] the algorithms are suitable for Smart Metering Systems.

10. Obligations and Notes for the Usage of the TOE

Table 1: Deliverables of the TOE outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

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

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

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

11. Security Target

For the purpose of publishing, the Security Target [ST] of the TOE is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AGD	Guidance Documents
AIS	Application Notes and Interpretation of the Scheme
ALC	Life-Cycle Support
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLS	Controllable Local System
CM	Configuration Management
CMC	CM Capabilities
CMS	Cryptographic Message Syntax
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
GWA	Gateway Administrator
HAN	Home Area Network
HGP	HTTP Gateway Protocol
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LED	Light-emitting diode
LMN	Local Metrological Network
LTE	Long Term Evolution – Mobile Radio Communication Standard
MAC	Message Authentication Code
NTP	Network Time Protocol
PII	Personally Identifiable Information
OBJ	Security Objectives
OPE	Operational User Guidance
OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
PRE	Preparative Procedures
SAR	Security Assurance Requirement
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SFR	Security Functional Requirement
SMGW	Smart Meter Gateway
ST	Security Target
TLS	Transport Layer Security Protocol
TOE	Target of Evaluation
TR	Technische Richtlinie - Technical Guideline
TSF	TOE Security Functionality
WAN	Wide Area Network

13.2. 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.

Commodity - Electricity, gas, water or heat

Consumer - End user of electricity, gas, water or heat

Controllable Local System – CLS are systems containing IT-components in the Home Area Network (HAN) of the consumer that do not belong to the Smart Metering System but may use the Gateway for dedicated communication purposes. CLS may range from local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to applications in home automation.

Energy Service Provider - Organisation offering energy related services to the consumer

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.

Home Area Network – In-house LAN which interconnects domestic equipment and can be used for energy management purposes

Informal - Expressed in natural language.

Meter - The term Meter refers to a unit for measuring the consumption or production of a certain commodity with additional functionality. It collects consumption or production data and transmits this data to the Gateway. As not all aspects of a Smart Meter are implemented in the descriptions within this document the term Meter is used. The Meter has to be able to encrypt and sign the data it sends and will typically deploy a Security Module for this. Please note that the term Meter refers to metering devices for all kinds of commodities.

Meter Data - Meter readings that allow calculation of the quantity of a commodity, for example electricity, gas, water or heat consumed or produced over a period. Other readings and data may also be included (such as quality data, events and alarms).

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

Personally Identifiable Information – Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

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.

Security Module - A Security device utilised by the Gateway for cryptographic support – typically realised in form of a smart card. The complete description of the Security Module can be found in [SM-PP].

Service Technician - Human entity that is responsible for diagnostic purposes.

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

Smart Metering System - The Smart Metering System consists of a Smart Meter Gateway and connected to one or more meters. In addition, CLS (i.e. generation plants) may be connected with the gateway for dedicated communication purposes.

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.

14. Bibliography

- [EUCC-VO] [Implementing Regulation \(EU\) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation \(EU\) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme \(EUCC\)](#) and [Implementation Regulation \(EU\) 2025/2462 of 8 December 2025 amending Implementing Regulation \(EU\) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document](#)
- [CC] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
<https://www.commoncriteriaportal.org>
- [CEM] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
<https://www.commoncriteriaportal.org>
- [EUCC_SOTA] EUCC state-of-the-art documents:
https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en
- [EUCC_PROG] EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), <https://www.bsi.bund.de/zertifizierung>
- [EUCC_CERT] EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (<https://certification.enisa.europa.eu/>) but also on BSI's website (<https://www.bsi.bund.de/zertifizierungsberichte>)
- [AIS] [Application Notes and Interpretations of the Scheme \(AIS\) as relevant for the TOE⁶](#) <https://www.bsi.bund.de/AIS>

⁶specifically

- AIS 1, Version 14, 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

[ST]	Security Target BSI-DSZ-CC-0822-V8-2026, Version 1.222, 2026-07-10, Security Target Smarty IQ-LTE, Sagemcom Dr. Neuhaus GmbH
[PP]	Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014, Bundesamt für Sicherheit in der Informationstechnik
[SM-PP]	Protection Profile for a Security Module for Smart Metering Systems, Version 1.03, 11 December 2014, BSI-CC-PP-0077-V2-2015, Bundesamt für Sicherheit in der Informationstechnik
[ETR]	Evaluation Technical Report Summary, Version 3, 2026-09-08, TÜV Informationstechnik GmbH (confidential document)
[ConfList]	Configuration list for the TOE (confidential documents): filelist_OS, 2026-07-14 filelist_sln8209, 2026-07-14 8209SE030_SMGw_Basis_LTE, Version 1.3, 2023-05-31 8209SE011_SMGw_CPU_USB, Version 3.3, 2022-03-24 8209SE040_SMGw_Basis, Version 1.4 2023-10-16 8209SE041_SMGw_Basis, Version 1.4 2023-10-16 Strukturstückliste nach Komponentenartikel 821014 Variante 1, 2021-08-04 Strukturstückliste nach Komponentenartikel 821014 Variante 1 V2.0, 2024-07-31 Strukturstückliste nach Komponentenartikel 821038 Variante 1, 2024-07-31 Strukturstückliste nach Komponentenartikel 821045 Variante 1, 2024-07-31 Documentation according to: Lebenszyklusunterstützung, Kap. 8.4.2 Dokumentation, Version 1.206, 2024-10-24, Sagemcom Dr. Neuhaus GmbH
[AGD_OPE]	Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb, Version 1.202, 2024-10-14, Sagemcom Dr. Neuhaus GmbH
[AGD_PRE]	Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen, Version 1.203, 2024-10-14, Sagemcom Dr. Neuhaus GmbH
[ALC_SichereLieferkette]	Sichere Lieferkette, Version 1.200, 2025-05-06, Sagemcom Dr. Neuhaus GmbH
[AGD_HGP]	Anlage zum AGD: HGP 2.5 SMGW - Http Gateway Protocol, Version 2.5.215, 2024-10-11, Sagemcom Dr. Neuhaus GmbH
[AGD_Audit]	Anlage zum AGD: Übersicht der Audit Records, Version 1.205, 2024-10-11, Sagemcom Dr. Neuhaus GmbH
[AGD_Record]	Anlage zum AGD: Übersicht der versendeten Events, Version 1.205, 2024-10-11, Sagemcom Dr. Neuhaus GmbH
[VulHand]	Schwachstellenmanagement und Offenlegung von Schwachstellen, Version 1.0, 2026-07-16, Sagemcom Dr. Neuhaus (confidential document)
[MSB-LK]	BSI. Anforderungskatalog zur MSB-Lieferkette, in der aktuell gültigen Fassung. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/MSB/MSB_node.html (cit. on pp. 38, 47). 2024, German Federal Office for Information Security
[FIPS-180-4]	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
- [RFC2104] Minimal Encapsulation within IP, October 1996
- [RFC2616] RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1 (<http://www.w3.org/Protocols/rfc2616/rfc2616.html>).
- [RFC4493] RFC4493 - The AES-CMAC Algorithm, JH. Song, R. Poovendran, J. Lee, T. Iwata, June 2006 (<https://tools.ietf.org/html/rfc4493>)
- [RFC5084] RFC5084 - Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), R. Housley, November 2007 (<https://tools.ietf.org/html/rfc5084>)
- [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>)
- [RFC5288] AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008
- [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>)
- [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>)
- [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>)
- [RFC5905] RFC5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification, D. Mills et al., June 2010 (<https://tools.ietf.org/html/rfc5905>).
- [RFC6033] Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type, December 2010
- [RFC6090] Fundamental Elliptic Curve Cryptography Algorithm, February 2011
- [RFC6161] Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type, April 2011
- [RFC723X] RFC 7230-7237 - Hypertext Transfer Protocol (HTTP/1.1)
- [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
- [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)
- [TR-02102-2] Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2026-01, Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109] Technische Richtlinie BSI TR-03109, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten

	Messsystem, Version 2.0.1, 2025-12-08, Bundesamt für Sicherheit in der Informationstechnik
[TR-03109-1]	Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 2.0, Datum 13.12.2024, Bundesamt für Sicherheit in der Informationstechnik.
[TR-03109-2]	Technische Richtlinie BSI TR-03109-2 Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1, Datum 15.12.2014, Bundesamt für Sicherheit in der Informationstechnik.
[TR-03109-3]	Technische Richtlinie BSI TR-03109-3, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1, 2014-04-17
[TR-03109-4]	Technische Richtlinie BSI TR-03109-4 Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways, Version 1.2.1, Datum 09.08.2017, Bundesamt für Sicherheit in der Informationstechnik
[TR-03109-1-I]	Technische Richtlinie BSI TR-03109-1 Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur, Version 1.0.9, Datum 12.2019, Bundesamt für Sicherheit in der Informationstechnik.
[TR-03109-1-IV]	Technische Richtlinie BSI TR-03109-1 IV: Feinspezifikation „Drahtgebundene LMN-Schnittstelle“, Version 1.0, Datum 18.03.2013, Bundesamt für Sicherheit in der Informationstechnik.
[TR-03109-1-VI]	Technische Richtlinie BSI TR-03109-1 Anlage VI: Betriebsprozesse, Version 1.0, Datum 18.03.2013, Bundesamt für Sicherheit in der Informationstechnik.
[TR-03111]	BSI - Technical Guideline, Elliptic Curve Cryptography, Version 2.10, 2018-06-01, Bundesamt für Sicherheit in der Informationstechnik
[TR-03116]	Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, Stand 2025, 2024-12-13
[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

C. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.