Federal Office
for Information Security

Certification Report

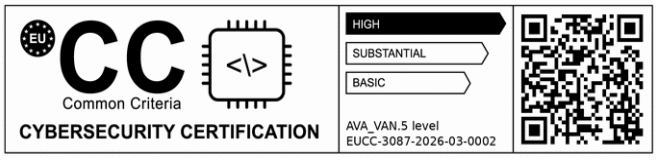
EUCC-3087-2026-03-0002
Administration ID
BSI-DSZ-CC-1000-V3-2026

for

Secure Smart Grid Hub (SGH-S) Version 2.00

from

EFR GmbH



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

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

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

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

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 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.
- The TOE Secure Smart Grid Hub (SGH-S), Version 2.00 has been re-certified by the certification body of the Federal Federal Office for Information Security (BSI) based on

[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

administration ID BSI-DSZ-CC-1000-V2-2025. Specific results from the evaluation process were re-used.

- The evaluation of the product Secure Smart Grid Hub (SGH-S), Version 2.00 was carried out by SRC Security Research & Consulting GmbH, located at
  Emil-Nolde-Straße 7
  53113 Bonn
  Deutschland.
- The evaluation was completed on 9 March 2026. SRC Security Research & Consulting GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: EFR GmbH.
- The assessed TOE was developed by: EFR 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 20 March 2026 is valid until 19 March 2034 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 positive 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 Secure Smart Grid Hub (SGH-S), Version 2.00 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.

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

[5] EFR GmbH
Nymphenburger Straße 20b
80335 München

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) is the Gateway in a Smart Metering System consisting of the SMGW Software, Version 2.0 and the SMGW Hardware, Versions SGH-S-AL1-B-200 or SGH-S-AM1-B-200. The TOE is comprised of a hardware board and an application software. Other hardware such as the hardwired security module (separately certified, BSI-DSZ-CC-1217-2024) or the communication modem is not part of the TOE.

It serves as the communication unit between devices of private and commercial consumers and commodity industry service providers (e.g. electricity, gas, water). It also collects, processes and stores Meter Data and is responsible for the distribution of this data to external entities.

Typically, the Gateway will be placed in the household or premises of the consumer of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g., power generation plants, controllable loads such as air condition and intelligent household appliances).

The product Secure Smart Grid Hub (SGH-S), Version 2.00 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 the product with the administration ID BSI-DSZ-CC-1000-V2-2025. Specific results from the evaluation process of the administration ID BSI-DSZ-CC-1000-V2-2025 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product Secure Smart Grid Hub (SGH-S), Version 2.00 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 9 March 2026. SRC Security Research & Consulting 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: AVA_VAN.5 and ALC_FLR.2

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

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

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

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

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

2. Identification of the TOE

The Information and communications technology product is identified as follows:

Secure Smart Grid Hub (SGH-S), Version 2.00

Holder of the certificate: EFR GmbH
Nymphenburger Straße 20b
80335 München
https://www.efr.de/en/contact/cybersecurity/

The following table outlines the TOE deliverables:

#	Type	Identifier	Release	Form of Delivery
1	HW	EFR Secure Smart Grid Hub v2.0	SGH-S-AL1-B-200 SGH-S-AM1-B-200	As a single device in a secure transport box by service technician
2	SW	TOE firmware, including bootloader, operating system, root file system and SMGW application	V2.0	Included in #1
3	DOC	Servicetechniker Handbuch für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S [AGD_PRE]	v2.01; 24.11.2025 SHA256 checksum 90508EC031BB6BA869AE3A2 2316FB746236BF5B976C7CF7 F936BD12673054982	Download
4	DOC	Produkthandbuch GWA für den Smart Meter Gateway Administrator (GWA) für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S [AGD_OPE]	v2.03; 20.11.2025 SHA256 checksum 15CA28DA1F7714663CD060D 3EA5F2BF581075A57CC66951 C6040BB81FD0934B0	Download
5	DOC	Handbuch für Endnutzer für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S	v2.01; 20.11.2025 SHA256 checksum 6E5B10837FF96433E582243B 6B3B516E39167B683CD2278C FB8499BD8D296193	Download

Table 1: Deliverables of the TOE

3. Security Policy

The TOE is delivered and installed by the service technician, who follows a defined, secured delivery plan.

Please note that the developer's responsibility for secure delivery ends with handing the TOE to a representative of the MPO (metering point operator), who is expected to deploy the TOE at its final destination. The representative may be the service technician or another member of the MPO's supply chain.

Alternatively, the MPO can define a delivery chain according to [MSB-LK].

Electronic documents: Download from the developer, the authenticity can be verified by the SHA256 checksum listed in [ST] and table 1.

The firmware is pre-installed in the TOE at production. No firmware installation is necessary or possible on installation by the service technician.

4. Assumptions and Clarification of Scope

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

OE.ExternalPrivacy: Authorized and authenticated external entities receiving any kind of private or billing-relevant data shall be trustworthy and shall not perform unauthorized 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 authorized individuals may physically access the TOE.

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

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

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

The Security Module shall be certified according to [SecMod-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 authorized external entity shall undergo a certification pro-cess according to this Security Target before they are issued to show that the update is implemented correctly. The external entity that is authorized 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 [BSI-TR-03109-3]. It shall also be ensured that the keys are brought into the Gateway in a secure way by the Gateway Administrator.

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

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

5. Architectural Information

The TOE is a single device that is part of a smart metering system. It is typically installed next to one or more meters for a commodity (e.g. electricity, water), to which it has wired or wireless connections.

It is either connected to a communications network (WAN, e.g. an internet router) or uses a cellular service. Over the WAN, it communicates with the Gateway Administrator or transfers consumption data to authorized entities. Locally, the consumer or a service technician can connect a device (e.g. a laptop) to access consumption or diagnostics data to which they are entitled.

The TOE contains a security module which is certified separately, and which provides crypto-graphic services to the TOE.

The TOE, its security module and communication electronics (except antennae) are contained in a plastic housing that is sealed to make manipulation attempts obvious.

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.

The developers website as stated in chapter 2 provides the following supplementary information:

- The product will be maintained during the validity of its certificate.
- Contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers: https://www.efr.de/kontakt/cybersecurity/
- Vulnerabilities are listed on ENISA's European Vulnerability Database (EUVD): https://euvd.enisa.europa.eu/

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: SRC Security Research & Consulting GmbH,
Emil-Nolde-Straße 7
53113 Bonn
Deutschland

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 in testing.

The software part of the test environment comprises

• test control program to interpret the developer's test scripts and generates test reports

• supporting test library

• hardware API

• software simulators

• interface and network configuration

• simulation software

On this basis, activity at the TOE's interface can be generated and the TOE's reaction observed. Also, the TOE's inner state can be manipulated (e.g. configuration, failures).

The test cases consist of preconditions, test steps, and expectations. The test scripts are formulated in the Robot Framework scripting language. The scripts are directly executable by the test environment, but also human readable. This is achieved by defining so-called keywords, which trigger specific actions, but also convey their meaning to the human reader.
The evaluator checked for the successful execution of the developer's functional tests and found no deviations.

The independent testing was performed using the developer’s testing environment. The configuration of the TOE being intended to be covered by the current evaluation was tested. The overall test result is that no deviations were found between the expected and the actual test results.

For the penetration testing firstly publicly known vulnerabilities have been collected from CVE database, textbooks and scientific publications. The applicability of each attack paths has been considered for the configured TOE in the indented environment.
In part II of the penetration analysis the evaluator analysed the CC deliverables for potential vulnerabilities already during the evaluation work for the corresponding aspects. The evaluators found no exploitable vulnerabilities in the evaluation deliverables.

Furthermore, in part III the evaluator used the potential vulnerabilities from the JIL document as the lead for further investigations. All possible attack methods against an authentic operational TOE are analysed. Thereby the results and experience of the JIWG working group consolidated in [JIL AttMeth] were taken into account.

The next discussion in part IV addressed the life cycle phases of the TOE. It provides an explanation why potential vulnerabilities cannot be exploited during the phases: development, production, installation and normal operation.

In part V a discussion was made on which technical level (hardware, various protocol levels of the external interface) an attacker might try an attack and why no vulnerabilities remain on each level.

In part VI a discussion was made based on the assets defined in [ST] and why no vulnerabilities remain, which were not already covered in the previous parts on each level.

Furthermore, the last part refers to the penetration tests, performed by the evaluators. 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 as defined in [ST] provided that all measures required by the developer are applied.

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

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

The developer provides type codes that unambiguously distinguish the TOE from related products and identifies the (non-TOE) communications parts. There is no difference in the security functionality between the type codes. Valid type codes are

- SGH-S-AL1-B-200
- SGH-S-AM1-B-200

Table 2: type codes

	Name	Power supply	Communications	HAN-CLS connection	Certification	Hardware-Version
Identifier	SGH-S-	A	L or M	1	-B	-200
Meaning	Smart Grid Hub – Secure	230 V AC	L: Ethernet and CAT1 LTE cellular radio M: Ethernet and CAT M1/NB2 LTE cellular radio	Ethernet-Switch HAN-CLS	Security Module, CC conformant, PTB A 50.8 approved	v2.00

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports [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].

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-3087-2026-03-0002, administration ID BSI-DSZ-CC-1000-V3-2026
- was issued on: 20 March 2026
- is valid until: 19 March 2034

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

9.2. Results of cryptographic assessment

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

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
Key generation	TLS-PRF with SHA-256 or SHA-384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	RFC 5289 RFC 5246(AES)	128 bit 256 bit	[BSI-TR-03116-3] [BSI-TR-03109-3]	2029+
Symmetric encryption, Integrity protection	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	RFC 5289 RFC 5246, FIPS 197 (AES) NIST SP800-38D(AES-GCM) NIST SP800-38A(AES_CBC) RFC-2104(HMAC)	128 or 256 bit	[BSI-TR-03109-3]	2029+
ECKA-EG key agreement and key derivation	ElGamal Key Agreement (ECKA-EG): ecka-eg X963KDF-SHA256 ecka-eg X963KDF-SHA384 ecka-eg X963KDF-SHA512	TR-03111, §4.1.3 TR-03111, $4.3.3 by usage of the security modules services	128 bit 192 bit 256 bit	[BSI-TR-03109-3]	2029+
AES key	Advanced Encryption	RFC-3394	128 bit	[BSI-TR-	2029+

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
wrap/ unwrap	Standard (AES) Key Wrap Algorithm with AES-ECB: id-aes128-wrap id-aes192-wrap id-aes256-wrap	FIPS 197	192 bit 256 bit	03109-1-I]	
Key generation	Generation of symmetric AES keys	TRNG Class 3	128 bit 192 bit 256 bit	[BSI-TR-03109-3] [BSI-TR-03109-1-I]	2029+
Encryption + Integrity protection	AES_GCM	FIPS Pub. 197 NIST-SP800-38D RFC 5084	128 bit 192 bit 256 bit	[BSI-TR-03109-3] [BSI-TR-03109-1-I]	2029+
Decryption + Integrity protection	AES_GCM AES_CBC_CMAC	FIPS Pub. 197 NIST-SP800-38D RFC 5652	128 bit 192 bit 256 bit	[BSI-TR-03109-3] [BSI-TR-03109-1-I]	2029+
Key generation	Key-generation of the shared secret via TRNG of the security module Key derivation of MK' for symmetrical encryption/decryption and integrity protection via AES-CMAC Key-generation for the TLS session according to FCS_CKM.1.1/TLS	TRNG Class 3	MK `and keys for symmetrical encryption/decryption: 128 bit TLS: Accord-ing to FCS_CKM.1.1/ TLS	[BSI-TR-03109-3] [BSI-TR-03116-3 §7.1.1]	2029+
Symmetrical encryption /decryption and integrity protection	AES-CMAC	BSI TR 03116-3 §7.2 RFC 4493	128 bit	[BSI-TR-03109-3] [BSI-TR-03116-3 §7.2]	2029+
Encryption, Decryption	AES_CBC	FIPS-197 ISO/IEC 18033-2:2006	128 bit	[BSI-TR-03109-3]	2029+
Integrity protection	AES-CMAC	FIPS-197 RFC4493	128 bit	[BSI-TR-03109-3]	2029+
Key destruction	Key overwriting and NV memory zeroization	-	-	-	2029+

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
Strong hash	SHA-256 SHA-384 SHA-512	FIPS-180-4	-	[BSI-TR-03109-3]	2029+
Encryption, Decryption	AES_256_XTS	IEEE 1619	2 keys each 256	[BSI-TR-02102]	

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 52, Para. 4, Clause 2).

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 their 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 their risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

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

11. Security Target

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

11.1. Acronyms

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CBC Cipher Block Chaining Mode

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM	Common Methodology for Information Technology Security Evaluation
CMS	Cryptographic Message Syntax
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECKA	ElGamal Key Agreement
ETR	Evaluation Technical Report
GCM	Galois/Counter Mode
GWA	Gateway Administrator
HAN	Home Area Network
HMAC	Keyed- Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and communications technology
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LMN	Local Metrological Network
LTE	Long Term Evolution
MAC	Message Authentication Code
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
SHA	Secure Hash Algorithm
SMGW	Smart Meter Gateway
SMPF	Smart Metering Platform Framework
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

11.2. 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.

12. 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/zertifizierungsreporte)
[AIS]	Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6] https://www.bsi.bund.de/AIS
[ST]	Security Target SMART GRID HUB – SECURE BSI-DSZ-CC-1000-V3-2026, Version 2.02, 30.01.2026, EFR GmbH
[PP]	Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014, BSI
[PP_Int]	Interpretationen und Festlegungen zum Schutzprofil „CC Protection Profile: Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, BSI-CC-PP-0073-2014, BSI
[SecMod-PP]	Protection Profile for the Security Module of a Smart Meter Gateway, Version 1.03, 11.12.2014, BSI-CC-PP-0077-V2, BSI
[ETR]	Evaluation Technical Report Summary, Version 3.0.1, 11.03.2026, SRC Security Research & Consulting GmbH (confidential document)
[IAR]	Impact Analysis Report, v1.20, 21.01.2026, EFR GmbH
[ConfList]	Konfigurations-Management-Scope Konfigurationsliste, v2.01_e, 30.01.2026, EFR GmbH (confidential document)
[DEL]	Auslieferungsprozess, v1.41_d, 19.10.2022, EFR GmbH
[MSB_DEL]	Ergänzungen bzw. Änderungen am ST für die Hinzunahme der MSB-Lieferkette, 21.11.2024, BSI
[MSB-LK]	Anforderungskatalog zur MSB Lieferkette, MSB-Lieferkette, Version 1.0, 2024, BSI
[AGD_PRE]	Servicetechniker Handbuch für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S; EFR, v2.01, 24.11.2025, EFR GmbH
[AGD_OPE]	Produkthandbuch GWA für den Smart Meter Gateway Administrator (GWA) für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S, v2.03, 20.11.2025, EFR GmbH
[AGD_CON]	Handbuch für Endnutzer für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S, v2.01, 20.11.2025, EFR GmbH
[PROD_INFO]	Smart Grid Hub – Secure, SGH-S Hoch sicheres Kommunikationsgateway für intelligente Messsysteme — Produktinformation, 11.01.2024, EFR GmbH

[6] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 48, Version 1.0, Anforderungen an die Prüfung von Sicherheitsetiketten

[JIL_AttMeth] Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, Version 2.3, January 2019, Joint Interpretation Working Group

[TR-02102] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

[TR-03109] BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb

[TR-03109-1] BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems; Version 1.0.1; 17.09.202116.01.2019

[TR-03109-2] BSI TR-03109-2 Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls; Version 1.1; 15.12.2014

[TR-03109-3] TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen; Version 1.1; 17.04.2014

[TR-03109-4] BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways; v.1.2.1; 09.08.2017

[TR-03116-3] BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme; 11.12.2019

[TR-03111] BSI TR-03111, Elliptic Curve Cryptography (ECC), Version 2.10, 2018, German Federal Office for Information Security [FIPS 180-4] NIST FIPS PUB 180-4: Secure Hash Standard (SHS). NIST, 2015.

[FIPS 197] NIST FIPS PUB 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES). NIST, 2001.

[NIST SP800-38A] NIST SP800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST, 2001

[NIST SP800-38D] NIST SP800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST, 2007.

[RFC 2104] Network Working Group RFC 2104, H. Krawczyk et al.: HMAC: Keyed-Hashing for Message Authentication. Network Working Group, Feb. 1997

[RFC 3394] IETF RFC 3394, J. Schaad, R. Housley: Advanced Encryption Standard(AES) Key Wrap Algorithm. IETF, 2002.

[RFC 4493] IETF RFC 4493, J. H. Song, J. Lee, T. Iwata: The AES-CMAC-Algorithm. IETF, 2006

[RFC 5084] IETF RFC 5084, R. Housley: Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS). IETF, 2007.

[RFC5246] RFC 5246 - The Transport Layer Security (TLS) Protocol, Version 1.2, Dierks & Rescorla - Standard Track, August 2008

[RFC 5289] IETF RFC 5289, E. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM). IETF, 2008

[RFC 5652] IETF RFC 5652, R. Housley, Cryptographic Message Syntax (CMS), 2009

[ISO/IEC 18033-2:2006] Information technology - Security techniques – Encryption algorithms - Part 2:Asymmetric ciphers, 2006

[IEEE 1619] IEEE 1619-2018, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, 2018

C. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report