Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1000-2023

for

Secure Smart Grid Hub (SGH-S) V1.00

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 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1000-2023 (*)

Smart Meter Gateway

Secure Smart Grid Hub (SGH-S)
V1.00

from	EFR GmbH
PP Conformance:	Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2
valid until:	10 September 2031

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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

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

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

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

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

Bonn, 11 September 2023

For the Federal Office for Information Security

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

Matthias Intemann L.S.
Head of Section

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

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

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

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

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

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

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

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

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

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

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

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies

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

of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

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

The product Secure Smart Grid Hub (SGH-S), V1.00 has undergone the certification procedure at BSI.

The evaluation of the product Secure Smart Grid Hub (SGH-S), V1.00 was conducted by SRC. The evaluation was completed on 6 September 2023. SRC is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: EFR GmbH.

The product was developed by: EFR GmbH.

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

5. Validity of the Certification Result

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

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

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

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 11 September 2023 is valid until 10 September 2031 combined with a regular mandatory re-assessment after every 2 years. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

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

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

6. Publication

The product Secure Smart Grid Hub (SGH-S), V1.00 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] EFR GmbH
Nymphenburger Straße 20b
80335 München

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the Gateway in a Smart Metering System consisting of the SMGW Software, Version 1.0 and the SMGW Hardware, Versions SGH-S-AL1-B-100 or SGH-S-AM1-B-100. The TOE is comprised of a hardware board and an application software. Other hardware such as the hardwired security module (separatly certified, BSI-DSZ-CC-1003-2018) 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 Security Target [6] 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 [8].

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

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

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

TOE Security Functionality	**Addressed issue**
Cryptographic Functionality	All cryptographic primitives (demanded in BSI TR 03116-3) required by the protocols as well as other services in the TOE are fully implemented in the TOE, including key exchange, key transportation, block cipher AES and hash functions. A security module according to BSI-CC-PP-0077-V2-2015 is used to generate cryptographic keys and digital signatures.
TLS Handling	The TLS protocol ensures the confidentiality and integrity of transmitted user data, most importantly the meter data and derived consumption information. The management inter-face is also protected by TLS.
Identification, Authentication And Authorization	The TOE contains a firewall and an access control management. The firewall enforces an information flow control policy based on BSI-CC-PP-0073. Communication that passes the firewall is handled by the access control management. Data access for each user is restricted to data which is explicitly assigned to this user. The TOE maintains the correct system time, so time-dependent data can be reliably

TOE Security Functionality	Addressed issue
	time-stamped
Self-Protection	The TOE periodically performs a self-test to detect malfunction or manipulation. This includes a data integrity check (including the TSF itself) using checksums and the evaluation of logging entries. This test can also be started by a user request. If a potential security violation is detected, the Gateway Administrator is informed. The TOE keeps separate system, consumer and calibration logs. The logs are protected against unauthorized access and deletion.
Security Management	A security management system is implemented in the TOE in order to preserve the security functionality in any case. The security functionalities of the TOE are protected against intentional and unintentional manipulation by a user. Therefore, all users are assigned to security roles and provided with security attributes. Following roles are available in the TOE: - Authorized consumer - Authorized gateway administrator - Authorized service technician - Authorized External Entity (FMT_SMR.1). The gateway administrator can provide firmware updates to the TOE. These updates must be cryptographically signed.

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Secure Smart Grid Hub (SGH-S), V1.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Secure EFR Smart Grid Hub	SGH-S v1.00	As a single device in a secure transport box by service technician
2	SW	TOE firmware, including boot-loader, operating system, root file system and SMGW application	Bootloader c2e15873 Root File System 9ac7c6ce03 Operating System 93ef40da7c8f SMGW-App 6.1.1- b955543b4	Included in 1
3	DOC	Servicetechniker Handbuch für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S [11]	V1.19; 15.06.2023 SHA256 checksum 4137c4cdc38fedb9bad1c8b034ffd47d58a0830287bfb680c8453f08396ead97	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 [12]	V1.22; 05.07.2023 SHA256 checksum 6257d6b87ef1bb50aebe390a80945f9b14475621dcca61f6ad21db22c05e28c4	Download
5	DOC	Handbuch für Endnutzer für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S [13]	v1.07; 31.07.2023 SHA256 checksum 8a7547ac0623bb9b08be6e8c1c86a8860fcdee3825198b4acbfe12223fe5cd79	Download

Table 2: Deliverables of the TOE

2.1. Delivery items and associated delivery methods

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

- After production, the TOE instances are stored in secure transport boxes (pylocx“) with electronic locks. These boxes can only be opened by authorized persons using one-time codes.
- For transportation of TOEs, the service technician or other authorized persons also use secure boxes with one-time codes.
- Transport time of TOEs should be no more than 24 hours. If this cannot be achieved, the secure boxes with the TOEs must be brought into a secure storage facility for every stop of more than 60 minutes.
- Each delivery is announced with the following information: Type and serial number of the secure box; IDs of the delivered TOEs; time and expected duration of the delivery trip.
- The recipient of a TOE delivery must check the integrity and serial number of the box on receipt.
- The service technician receives at most 100 TOE devices in one delivery.
- The IDs of delivered TOEs are documented, so the identity of delivered and installed TOEs can be checked at all stages of the delivery process.

- In addition to that a personal handover by one employee (5 devices) or two employees (10 devices) is also possible.

Electronic documents: Download from the developer. The authenticity can be verified by the SHA256 checksum listed in [ST], sec. 1.2

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

2.2. Identification of the TOE by the User

For the customer and service technician to be able to check the correct delivery visually, instructions are provided in [11], [12] and [13].

Further checks by the user can be done as following on the installed TOE:

- the labeling of the housing, showing the name, type and serial number
- the consumer client software TRuDi can show the firmware version of the TOE

The electronic guidance documents can be identified by their SHA256 checksum listed in [6], section 1.2.

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: Protection of metrological data stored and transmitted from a non-public environment within the premises of the consumer providing a basic level of physical protection by implementing logical and additional physical security functionality

In addition, the TOE implements policies pertaining to the following security functional classes: Security Audit, Communication, Cryptographic support, User Data Protection, Identification and Authentication, Security Management, Privacy, Protection of the TSF and Trusted path/channel.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Trustworthy authorised and authenticated external entities
- Trustworthy and well-trained gateway administrators and service technicians
- Basic level of physical protection by installation in a non-public environment within the premises of the consumer
- Processing profiles are obtained from a trustworthy and reliable source only
- Usage of a certified Security Module for specific cryptographic services
- Certification of firmware updates prior to installation in the SMGW
- Reliability and availability of WAN network connections, trustworthiness and availability of time sources, assumptions on LMN and HAN network connections
- Secure generation of ECC key pair and secure transmission to SMGW by the GWA

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

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.

The TOE is structured into 45 subsystems that can be reduced into 10 logical units.

Hardware: Includes seals, housing, and the electronic logic board and guarantees passive physical protection of the TOE.

Operating System: The underlying operating system including encryption and integrity protection for bootloader, kernel and the SMGW application. Provides network-services, firewall functionality and user-separated access control.

Administration: Gives access for trusted and authorized users for administration, management of processing profiles, and access to log-files.

Notification: Sends notifications to trusted users to inform about critical events.

Integrity Protection: Includes all functionality to guarantee the integrity of the TOE, including constant monitoring of the TOEs filesystem, data-integrity, availability of HW resources and execution of self-tests.

Cryptography: Provides cryptographic services and implements access to the SMGWs security module.

LMN: Contains the communication with wired and wireless LMN participants and their configuration as well as the tariffication according to the processing profiles.

HAN: Allows access for trusted and authorized end-users to access energy consumption and audit data.

CLS: Implements communication channels for CLS devices

System Services: Provides further services to the SMGW application including NTP and management of the mobile communication.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

7. IT Product Testing

The developer used mostly automated tests for their functional testing, supplemented by some manual tests where automation was not feasible. Each test focused on with a specific part of the TSF, but since the tests are integration tests, the whole TOE was always the target. A single configuration of the TOE exists and is intended to be covered by this evaluation.

The test cases are mapped to the interfaces described in the functional specification. Each TSFI is tested in at least one test case and therefore the correspondence between the interfaces in the functional specification and the tests in the test documentation is complete.

The evaluator added some test cases to complement the developer's test coverage. Those tests were incorporated in the developer's test suite and were subsequently executed during each development cycle. All tests were passed by the final TOE.

The evaluator performed penetration testing to assure that the TSF could not be circumvented. In special focus were vulnerabilities that allowed to bypass the encryption and authentication on the network ports. No vulnerabilities were found.

7.1. Developer’s Testing

There is only one configuration of the TOE. The use of different communication modules (LTE, wMBUS) is outside of the scope of this evaluation (see [6], section 1.3).

Developer’s Test Results

The developer manages their test results in TestRail. The evaluator exported the test results from there in the form of an CSV file. The resulting file is very similar to the test specifications, but the additional fields "Status" (the test result) and "Tested By" (the person who performed the test) and "Tested On" (date and time of the test) are included as evidence that the test has in fact been performed.

Verdict

All tests passed with the expected results.

7.2. Independent Testing

The independent testing was performed using the developer’s testing environment.

During ATE_COV and ATE_DPT, the evaluator had identified several tests to be added or modified to complete the developer's test coverage. Those tests were added to the developer's test repository and also repeated during ATE_IND.

Verdict

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

7.3. Penetration Testing

The evaluator searched methodically for vulnerabilities in the TOE. Notably, the evaluators

- looked for evidence for vulnerabilities while preparing the Single Evaluation Reports for the different evaluation aspects,
- checked for publicly known vulnerabilities in third-party and open source components of the TOE, and evaluated the developer responses to potentially exploitable vulnerabilities,
- evaluated the TLS implementation of the TOE for standard conformance and correctness,
- performed a side channel analysis within the limits of an local attacker,

- performed penetration testing to check if the authentication and access control of the TOE could be circumvented, and
- tested the TOE resistance against physical tampering.

The evaluators found no exploitable vulnerabilities.

Verdict

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the high attack potential was actually successful.

8. Evaluated Configuration

This certification covers the following configurations of the TOE. Only one TOE configuration exists, consisting of the items listed in table 2. Multiple Communication Modules for LTE exist, however these are non-TOE components and as such out of scope for this certification.

9. Results of the Evaluation

9.1. CC specific results

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

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

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

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

The evaluation has confirmed:

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

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

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 [16] BSI-TR-03109-3 [15]	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 [15]	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 [15]	2029+
AES Key wrap /unwrap	Advanced Encryption Standard (AES) Key Wrap Algorithm with AES-ECB: id-aes128-wrap id-aes192-wrap id-aes256-wrap	RFC-3394 FIPS 197	128 bit 192 bit 256 bit	BSI-TR-03109-1-I [14]	2029+
Key generation	Generation of symmetric AES keys	PTG.3	128 bit 192 bit 256 bit	BSI-TR-03109-3 [15] BSI-TR-03109-1-I [14]	2029+
Encryption + Integrity protection	AES_GCM	FIPS Pub. 197 NIST-SP800-38D RFC 5084	128 bit 192 bit 256 bit	BSI-TR-03109-1-I [14] BSI-TR-03109-3 [15]	2029+

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Validity Period
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 [15] BSI-TR-03109-1-I [14]	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	PTG.3	MK' and keys for symmetrical encryption/ decryption: 128 bit TLS: According to FCS_ CKM.1.1/TLS	BSI-TR-03109-3 [15] BSI-TR-03116-3 §7.1.1 [16]	2029+
Symmetrical encryption /decryption and integrity protection	AES-CMAC	BSI TR 03116-3 §7.2 RFC 4493	128 bit	BSI-TR-03109-3 [15] BSI-TR-03116-3 §7.2 [16]	2029+
Encryption, Decryption	AES_CBC	FIPS-197 ISO/IEC 18033-2:2006	128 bit	BSI-TR-03109-3 [15]	2029+
Integrity protection	AES-CMAC	FIPS-197 RFC4493	128 bit	BSI-TR-03109-3 [15]	2029+
Key Destruction	Key overwriting and non-volatile memory zeroization	-	-	-	
Strong Hash/ Integrity protection	SHA-256 SHA-384 SHA-512	FIPS-180-4	-	BSI-TR-03109-3[15]	2029+
Encryption, Decryption	AES_256_XTS	IEEE 1619	2 keys each 256 bit	BSI-TR-02102 [17]	2029+

Table 3: TOE cryptographic functionality

The strength of these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to TR-03116-3 [15] or TR-02102-1 [16], the algorithms are suitable for Smart Metering Systems.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cyber Block Chain
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 Cryptograph
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
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
WAN	Wide Area Network
TSF	TOE Security Functionality

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012, https://www.commoncriteriaportal.org

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

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

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

[6] Technical Specification Security Target Smart Grid Hub – Secure, BSI-DSZ-CC-1000-2023, Version 1.22, 06.09.2023, EFR GmbH

[7] Evaluation Technical Report Summary Secure Smart Grid Hub, Certification ID BSI-DSZ-CC-1000, Version 1.3.2, 06.09.2023, SRC Security Research & Consulting GmbH (confidential document)

[8] Protection Profile for the Gateway of a Smart Metering System, Version 1.3, 31 March 2014, BSI-CC-PP-0073-2014, 11.12.2014, German Federal Office for Information Security

[9] Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, BSI-CC-PP-0077-V2-2015, German Federal Office for Information Security

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 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

[10] CC Assurance Komponenten ALC_CMS “Konfigurations-Management-Scope Konfigurationsliste”, v1.13, 30.08.2023, EFR GmbH (confidential document)

[11] Servicetechniker Handbuch für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S, V1.19, 15.06..2023, EFR GmbH

[12] Produkthandbuch GWA für den Smart Meter Gateway Administrator (GWA) für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S, V1.22, 05.07.2023, EFR GmbH

[13] Handbuch für Endnutzer für das Smart-Meter-Gateway (SMGW) Secure Smart Grid Hub EFR SGH-S, v1.07, 31.07.2023, EFR GmbH

[14] Technische Richtlinie BSI TR-03109-1-I Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.1, 17. September 2021, German Federal Office for Information Security

[15] TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen; Version 1.1; 17.04.2014, German Federal Office for Information Security

[16] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, Stand 2023, 06.12.2022, German Federal Office for Information Security

[17] Technische Richtlinie BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2020-01, 04.03.2020, German Federal Office for Information Security

[18] Standard of Implementation:

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. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.4
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 11
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report