Federal Office
for Information Security

Certification Report

BSI-CC-PP-0073-V2-2024

for

Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0

developed by

Federal Office for Information Security

Federal Office for Information Security (BSI), Postfach 20 03 63, 53133 Bonn, Germany
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-CC-PP-0073-V2-2024

Common Criteria Protection Profile

Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0

developed by Federal Office for Information Security

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by
AVA_VAN.5, ALC_FLR.2

valid until 18 December 2034

SOGIS Recognition Agreement

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version CC:2022 for conformance to the Common Criteria for IT Security Evaluation (CC), Version CC:2022. 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 Protection Profile and in conjunction with the complete Certification Report.

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

Bonn, 19 December 2024
For the Federal Office for Information Security

Sandro Amendola
Director-General

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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 Act on the Federal Office for Information Security (BSIG), the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. A PP claimed by a user, consumer or stakeholder for IT gives them the possibility to express their IT security needs without referring to a specific product. Product certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued but the results from a PP certification can be re-used for the Security Target evaluation within a product evaluation when conformance to the PP has been claimed.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor. A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1]. The evaluation is usually 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.

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 (BSIG)[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte 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], including PP Certification
- 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
Current version see website: http://www.gesetze-im-internet.de/bsig_2009/index.html

[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
Current version see website: http://www.gesetze-im-internet.de/bsizertv_2014/index.html

[3] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365
Current version see website: https://www.bsi.bund.de/Gebuehrenverordnung

- Common Criteria for IT Security Evaluation (CC)[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Internal procedure for the issuance of a PP certificate

3 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of IT security certificates - as far as such certificates are based on CC - under certain conditions was agreed. Therefore, the results of this evaluation and certification procedure can be re-used by the product certificate issuing scheme in the evaluation of a Security Target within a subsequent product evaluation and certification procedure.

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 up to and including Common Criteria (CC) Evaluation Assurance Levels EAL 4, and in addition at higher recognition levels for IT-Products related to certain technical domains only. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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.

Details on recognition, the signatory nations, technical domains and the agreement itself can be found at https://www.sogis.eu.

3.2 International Recognition of CC – Certificates (CCRA)

The international Common Criteria Recognition Arrangement (CCRA) became effective in September 2014 in its current version. It defines the recognition of certificates for IT-products 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 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.

Details on recognition, the signatory nations and the agreement itself can be found at https://www.commoncriteriaportal.org.

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.

[4] Proclamation of the Federal Office for Information Security of 14 April 2023 on https://www.bsi.bund.de

The Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0 has undergone the certification procedure at BSI.

The evaluation of the Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0 was conducted by the ITSEF SRC Security Research & Consulting GmbH. The evaluation was completed on 18 December 2024. The ITSEF SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Federal Office for Information Security.

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 only applies to the version of the Protection Profile as indicated.

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

For the meaning of the CC concepts and terms please refer to CC [1] Part 1 through 5.

The validity of this certificate ends as outlined on the certificate. The applicant and the sponsor of this certificate are recommended to review the technical content of the Protection Profile certified according to the evolvement of the technology and of the intended operational environment of the type of product concerned as well as according to the evolvement of the evaluation criteria. Such review should result in an update and a re-certification of the Protection Profile accordingly. Typically, technical standards are reviewed on a five years basis.

The limitation of validity of this PP certificate does not necessarily impact the validity period of a product certificate referring to this Protection Profile, but the certification body issuing a product certificate based on this Protection Profile should take it into its consideration on validity.

6 Publication

The Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0 has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: https://www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

The Certification Report may be obtained in electronic form at the internet address stated above.

[5] Information Technology Security Evaluation Facility

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

The Protection Profile for a Smart Meter Gateway (SMGW-PP),Version 2.0 [5] is established by the Federal Office for Information Security as a basis for the development of Security Targets in order to perform a certification of an IT-product, the Target of Evaluation (TOE).

The Target of Evaluation (TOE) that is described in the evaluated Protection Profile is an electronic unit comprising hardware and software used for collection, storage and provision of Meter Data from one or more Meters of one or multiple commodities.

The SMGW connects a Wide Area Network (WAN) with a Local Metrological Network (LMN) of one or more Meters, and the Consumer Home Area Network (HAN), which hosts optional Controllable Local Systems (CLS). The security functionality of the TOE comprises

- protection of confidentiality, authenticity, integrity of data and
- information flow control

mainly to protect the privacy of consumers, ensure a reliable billing process, provide a secure channel to the CLS and protect the Smart Metering System and a corresponding large scale infrastructure of the smart grid.

The SMGW uses the services of a Security Module (e.g. a smart card) as a cryptographic service provider, as a random number generator and as secure storage for confidential assets. The Security Module will be evaluated separately according to the requirements in the corresponding Protection Profile. The Security Module is a different IT product and not part of the TOE as described in the PP. Nevertheless, it is physically embedded into the SMGW and protected by the same level of physical protection.

The availability of the SMGW is not addressed by the PP.

The PP utilizes a modular structure and specifies a base PP and two additional functional packages. The functional package “Power Limitation”, Version 1.0 shall be used if the TOE supports controlling of CLS directly in the following way: For a CLS, the GWA configures a controlling profile on the TOE. This controlling profile contains information such as the CLS identification, external entities associated with the CLS, information on the kind of commands sent to the CLS for controlling. The functional package “Multiple grid connection points”, Version 1.0 shall be used if the TOE is intended to be installed in an environment, where it cannot be assumed that all connected meters are covered by the same physical protection as the TOE. In particular, the bundling of devices of grid connection points with one TOE is permitted for grid connection points connected to one grid node of the same voltage level.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [5], chapter 3.2. Based on these assets the security problem definition is defined in terms of assumptions, threats and organisational security policies. This is outlined in the Protection Profile [5], chapter 3.3, chapter 3.4 and chapter 3.5, respectively. Due to the modular structure of the PP, the security problem definition can be changed in case a functional package is used. The functional package “Power Limitation” introduces additional assets, assumptions, threats and adjusts an OSP. This is defined in [5], chapter 7.2.3. The functional package “Multiple grid connection points” adjusts assumptions, threats and replaces the definition of the local attacker. This is defined in [7], chapter 1.4

These assumptions, threats and organisational security policies are split into security objectives to be fulfilled by a TOE claiming conformance to this PP and security objectives to be fulfilled by the operational environment of a TOE claiming conformance to this PP. These objectives are outlined in the PP [5], chapter 4. In the functional package “Power Limitation” some security objectives for the TOE are adjusted and an additional security objective for the environment is added. This is defined in [5], chapter 7.2.4. In the functional package “Multiple grid connection points” some security objectives for the environment are adjusted as defined in [7], chapter 1.5.

The Protection Profile [5] requires a Security Target or another PP based on the base PP or based on the base PP together with one functional package or both functional packages as defined in [5], Section 7.2.3 and in [7], respectively, claiming this PP to fulfil the CC requirements for strict conformance.

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of security functional requirements (SFR) to be implemented by a TOE. It covers the following issues: communication concealing, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of the TSF, trusted path/channels.

The functional package “Power Limitation” defined in [5] chapter 7.2 adapts SFRs related to user data protection and security management.

The functional package “Multiple grid connection points” defined in [7] adapts SFRs related to: Cryptographic support, Trusted path/channels, and introduces an additional optional SFR related for Protection of the TSF.

These TOE security functional requirements are outlined in the PP [5], chapter 5 and chapter 6 as well as in chapter 7.2 and in [7] chapter 1.7 for the respective functional packages. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by
AVA_VAN.5, ALC_FLR.2

(for the definition and scope of assurance packages according to CC see [1], part 3 for details).

The assurance requirement ALC_DEL was refined to enable the usage of the MSB-Lieferkette as defined in [8]. The assurance refinements outlined in the Protection Profile were followed in the course of the evaluation.

4 Results of the PP-Evaluation

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all Application Notes and Interpretations of the Scheme (AIS) [4] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE (Protection Profile evaluation).

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1.

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

- The Protection Profile contains application notes, the author of a product specific Security Target needs to consider when creating a Security Target and implementing a TOE that claims conformance to this PP.

6 Protection Profile Document

The Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0 [5] and the Annex to Protection Profile for a Smart Meter Gateway (SMGW-PP) - Functional Package Multiple Grid Connection Points, Version 1.0 [7] are being provided within separate documents as Annex A of this report.

7 Definitions

7.1 Acronyms

AIS Application Notes and Interpretations of the Scheme

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

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CLS Controllable Local System

EAL Evaluation Assurance Level

EMT Externer Marktteilnehmer

ETR	Evaluation Technical Report
GWA	Gateway Administrator
HAN	Home Area Network
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LMN	Local Metrological Network
MPO	Metering Point Operator
MSB	Messstellenbetreiber
PII	Personally Identifiable Information
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMGW	Smart Meter Gateway
SRV	Service Technician
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAN	Wide Area Network

7.2 Glossary

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

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

Controllable Local System - e.g. "local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to applications in home automation." [5], sec. 1.4.2

Externer Marktteilnehmer - External market participant; any recipient of SMGW data except the GWA.

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

Gateway Administrator - Authority responsible for administrating the gateway.

Home Area Network - Local network, possibly belonging to the Consumer or owner of the premises.

Informal - Expressed in natural language.

Local Metrological Network - Connection of the meters; either wired or wireless, within the premises of the Consumer.

Messstellenbetreiber – see: Metering Point Operator.

Metering Point Operator - Entity that is responsible for the installation and operation of SMGWs and meters.

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

Personally Identifiable Information - Information that can be attributed to an individual person and whose disclosure can violate the person's privacy.

Premises of the Consumer - The building where the Consumer consumes or produces commodities or another building in the immediate vicinity on the same property.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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

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

Service Technician - Installs, maintains and diagnoses the SMGW in the operating environment on behalf of the MPO.

Smart Meter Gateway - "Gateway"; the TOE of [5]

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

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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.

Wide Area Network - Transport network for communication with GWA and EMTs, e.g. "the internet".

8 Bibliography

[1] ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements

https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components

- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements

https://www.commoncriteriaportal.org

[2] ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
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[6].

[5] Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0, Bundesamt für Sicherheit in der Informationstechnik, 13.12.2024

[6] Evaluation Technical Report, Version 1.2, 11.12.2024, Evaluation Technical Report – Summary (ETR), SRC Security Research & Consulting GmbH (confidential document)

[7] Annex to Protection Profile for a Smart Meter Gateway (SMGW-PP) - Functional Package Multiple Grid Connection Points, BSI, Version 1.0, 13.12.2024

[8] Anforderungskatalog zur MSB-Lieferkette, BSI, Version 1.0, October 2024

[6] specially

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C Annexes

List of annexes of this certification report

Annex A: Protection Profile for a Smart Meter Gateway (SMGW-PP), Version 2.0 [5] provided within a separate document.

Annex to Protection Profile for a Smart Meter Gateway (SMGW-PP) - Functional Package Multiple Grid Connection Points, Version 1.0, [7] provided within a separate document.

Note: End of report