Federal Office
for Information Security

Annex to Protection Profile for a Smart Meter Gateway (SMGW-PP) - Functional Package Multiple Grid Connection Points

Version 1.0

13.12.2024

Bundesamt für Sicherheit in der Informationstechnik
PO Box 20 03 63
53133 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

List of Tables

1 Functional package: Multiple grid connection points

1.1 Package identification

Title	Multiple grid connection points functional package
Short title	MultipleGcpFp
Version	1.0
Date	This functional package inherits the date of the base PP. Please refer to [PP-0073] Section 1.2.
Sponsor	This functional package inherits the sponsor of the base PP. Please refer to [PP-0073] Section 1.2.
Registration	This functional package inherits the certification ID of the base PP. Please refer to [PP-0073] Section 1.2.
CC Version	CC:2022 Revision 1
Conformance claim	• The conformance of this package is Common Criteria ([CC]) Part II conformant • The conformance of this package is Common Criteria ([CC]) Part III conformant

Table 1.1 Identification of functional package multiple grid connection points

1.2 Package overview

This functional package depends on the base PP [PP-0073].

This functional package 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 threat model in [PP-0073] Chapter 3 does not cover this scenario; in particular, not all attack vectors of this scenario are addressed in the threat model of the base PP. Therefore, the following section describes a security problem definition for this use case of the TOE. Note that this security problem definition adds to the security problem definition of the base PP, and that this functional package shall only be used in combination with the base PP.

The ST author shall further adjust [PP-0073] Chapter 1 to address this use case.

1.3 Definition of terms

In the base PP, the networks HAN and LMN are considered to be in-house networks, see [PP-0073], Glossary. For the use case of this functional package, however, this consideration does not hold any more. The ST author shall therefore adjust the definition of these networks as follows.

Term	Description
HAN	Local data communication network which interconnects IT equipment with the SMGW and can e.g. be used for energy management purposes. The expansion of the network is restricted to the distance between SMGW and the properties with connected meters.
LMN	Local data communication network which connects meters with the SMGW. The expansion of the network is restricted to the distance between SMGW and the properties with connected meters.

Table 1.2 Adjustments to the glossary from the base PP for the functional package multiple grid connection points

1.4 Security problem definition

1.4.1 Assets

This package does not contain any additional assets.

1.4.2 Assumptions

The following assumptions shall be adjusted from the base PP if this functional package is chosen.

A.PhysicalProtection It is assumed that the TOE is installed

- either in a non-public environment within a closed facility with restricted access[1], which provides an enhanced-basic level of physical protection. This protection covers the TOE as well as the communication channel between the TOE and its security module,
- or in a public environment within a casing which provides an enhanced-basic level of physical protection for the TOE and which restricts direct access to the TOE. This protection covers the TOE as well as the communication channel between the TOE and its security module.

In both cases, it is assumed that the operational environment ensures that physical tampering of the TOE is detectable and that the GWA and the consumer are notified without undue delay in case physical tampering has occurred.

A.ExtensionLocalNetwork It is assumed that the spatial expansion of the networks HAN and LMN is restricted to the distance of the TOE to connected devices of bundled grid connection points. A bundling of grid connection points with one TOE is permitted provided that the grid connection points are connected to one grid node of the same voltage level.

1.4.3 Attackers

The definition of the local attacker in [PP-0073], Section 3.4 in the base PP shall be replaced by the following definition.

Local attacker: An attacker that

- either has physical access to meter, TOE, a connection between these components, or local logical access to any of the interfaces, who tries to disclose or alter assets while stored in the TOE or while transmitted between external entities and the TOE;
- or is located in the HAN or LMN and tries to disclose or alter assets transmitted via these networks.

Considering the limited value of information processed by a single TOE (resulting in a lower attack motivation in comparison to remote attacks on a large number of TOEs), the following threat model assumes for the vulnerability assessment, that local attackers ***have at most proficient expertise and use at most specialized equipment***. However, the preparation of local attacks in terms of developing the attack path including tools can be performed by attackers with full AVA_VAN.5 attack potential (i.e., multiple expert expertise and multiple bespoke equipment), as long as their execution is possible with the restrictions for local attackers mentioned above (also for all remote attacks (cf. following bullet point) the full AVA_VAN.5 attack potential has to be assumed during the vulnerability assessment).

Please note that the local attacker includes authorized entities like consumers or other entities having access to the environment where the TOE is located.

1.4.4 Threats

This package does not contain any additional threats. Note, however, that by adjusting the definition of the local attacker, all threats with the threat agent being a local attacker address a wider range of attack vectors. This concerns the following threats:

- T.DataModificationLocal
- T.TimeModification
- T.DisclosureLocal
- T.ResidualData

[1] This may also comprise the premises of the MPO.

- T.ResidentData

1.4.5 OSP

This package does not contain any additional OSPs.

1.5 Security objectives

1.5.1 Security objectives for the TOE

This package does not contain any additional security objectives for the TOE.

1.5.2 Security objectives for the environment

This package does not contain any additional security objectives for the environment. However, the following security objectives for the environment shall be adjusted from the base PP if this functional package is chosen.

OE.PhysicalProtection The TOE shall be installed

- in a non-public environment within a closed facility with restricted access that provides an enhanced-basic level of physical protection. This protection shall cover the TOE as well as the communication channel between the TOE and its security module.
- or in a public environment within a casing which provides an enhanced-basic level of physical protection for the TOE and which restricts direct access to the TOE. This protection shall cover the TOE as well as the communication channel between the TOE and its security module.

In both cases, the operational environment shall ensure that physical tampering of the TOE is detectable and that the GWA and the consumer are notified without undue delay in case physical tampering has occurred.

Application Note 1: The detection of physical tampering and notification of GWA and consumer may also be provided by the TOE itself, by fulfilling e.g. FPT_PHP.2 from [CC:2022] Part 2. The optional SFR FPT_PHP.2 as defined below should then be used additionally to FPT_PHP.1. If the security functionality is provided by the TOE, parts of this security objective have to be re-assigned to a security objective for the TOE, the SFR then mapping to that new security objective for the TOE. For more details, also concerning the partial removal of the respective assumption, see [CC:2022] Part 1, Sect. 10.6.

OE.ExtensionLocalNetwork The spatial expansion of the networks HAN and LMN shall be restricted to the distance of the TOE to connected devices of bundled grid connection points. A bundling of grid connection points with one TOE is permitted provided that the grid connection points are connected to one grid node of the same voltage level.

1.5.3 Security objectives rationale

Since no new threats, assumptions or OSPs, and no new security objectives have been added, the security objectives rationale and mapping remains as in the base PP. Where the assumptions have been adjusted, the corresponding security objectives for the environment have been adjusted analogously, as such, the rationale for the mapping is obvious.

1.6 Application notes

Per [CC:2022] Part 1 Annex 1, audit and management requirements relating to the SFRs of the subsequent section shall be specified in this section.

1.7 Security functional requirements

The following security functional requirements shall be *adjusted from or added to the base PP* if this functional package is chosen.

1.7.1 FCS_COP.1/MTRCMAC

FCS_COP.1.1/MTRCMAC has to be replaced as follows:

FCS_COP.1.1/ MTRCMAC The TSF shall perform [*MAC generation and verification for secure communication with meters*] in accordance with a specified cryptographic algorithm [*AES-CMAC*] and cryptographic key sizes [*128 bit with [selection: 96 bit truncated MAC, 128 bit untruncated MAC]*] that meet the following: [*[RFC4493]*].

1.7.2 FTP_PRO.*/SYM

The security functionality requirement is implicitly adjusted by the referenced SFR **FCS_COP.1/MTRCMAC**. The text of **FTP_PRO.*/SYM** remains unchanged.

1.7.3 FPT_PHP.2 (optional)

If FPT_PHP.2 is included in the package to address parts of A.PhysicalProtection, it has to be included as follows:

1.7.3.1 FPT_PHP.2: Notification of physical attack

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that can compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [*all TSF devices/elements*], the TSF shall monitor the devices and elements and notify [*the GWA, the consumer*] when physical tampering with the TSF's devices or TSF's elements has occurred.

Hierarchical to: FPT_PHP.1

Dependencies: FMT_MOF.1 unfulfilled, see Application Note below.

Application Note 2 When including FPT_PHP.2 in the ST, the ST author shall expand the table for FPT_FLS.1 in [PP-0073] to add the detection of intrusion by the TOE as in FPT_FLS.1 and the reaction of the TOE. Further, the ST author shall add the event "detection of intrusion" to all logs in FAU_GEN.1/*.

Note that even though FPT_PHP.2 is hierarchical to FPT_PHP.1, FPT_PHP.1 shall remain in the ST even if FPT_PHP.2 is chosen.

Application Note 3 As the users to be notified are fixed and as all TSF devices/elements shall be monitored, no management of these is necessary. Therefore, the dependency on FMT_MOF.1 remains unfulfilled. The ST author shall add this justification to the dependency table of the ST.

1.7.4 Security functional requirements rationale

As there are neither new nor adjusted security objectives for the TOE, the rationale of the base PP remains unchanged.

Application Note 4: If the optional SFR FPT_PHP.2 is included in the TOE, and parts of the security objective OE.PhysicalProtection are re-assigned to a security objective for the TOE, the rationale in the ST has to include the respective necessary mappings.

References

[CC:2022] *Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1.* CCDB/ISO.

[PP-0073] *BSI-CC-PP-0073-V2, v2.0 Protection Profile for a Smart Meter Gateway (SMGW-PP).* Bundesamt für Sicherheit in der Informationstechnik.

[RFC4493] *The AES-CMAC Algorithm.* IETF, TH Song, R. Poovendran, J. Lee and T. Iwata. 2006.