



Bundesamt
für Sicherheit in der
Informationstechnik

ERRATA FÜR DAS SMGW-SCHUTZPROFIL (BSI-CC-PP-0073 v1.3) ZUR UMSETZUNG VON TAF 9, 10 UND 14

Version 1.1, Datum 12.12.2019



1 Einleitung

2 Dieses Errata-Dokument befasst sich mit Interpretationen und Klarstellungen zu Anforderun-
3 gen des BSI-CC-PP-0073 an SMGWs. Insbesondere wird auf Anforderungen im Rahmen der
4 Umsetzung von TAF 9, 10 und 14 gemäß Errata zu TR-03109-1 v1.0.1 (siehe [TR-Er-
5 rata_TAF9_10], [TR-Errata_TAF14]) eingegangen.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27 2 Processing Profiles

28 Nach [BSI-CC-PP-0073] definieren „Processing Profiles“ wie Messwerte im Gateway verarbeitet
29 werden und an wen sie in welcher Form versendet werden müssen. Genauer:

30 *“A Processing Profile defines:*

- 31 • *how Meter Data must be processed,*
- 32 • *which processed Meter Data must be sent in which intervals,*
- 33 • *to which component or external entity,*
- 34 • *signed using which key material,*
- 35 • *encrypted using which key material,*
- 36 • *whether processed Meter Data shall be pseudonymised or not, and*
- 37 • *which pseudonym shall be used to send the data*

38 *The Processing Profiles are not only the basis for the security features of the TOE; they also contain*
39 *functional aspects as they indicate to the Gateway how the Meter Data shall be processed. More*
40 *details on the Processing Profiles can be found in [BSI-TR-03109-1].” [BSI-CC-PP-0073, 1.4.6.1]*

41 Damit dienen sie insbesondere für die Konfiguration der Tarifierungsanwendungsfälle (TAFs)
42 nach [BSI-TR-03109-1] (dort Auswertungsprofile genannt).

43 Processing Profiles stellen damit einen zentralen Punkt im Datenverarbeitungskonzept des
44 SMGWs dar und gehören im Sinne der CC zu den Assets, deren Integrität, Authentizität und
45 Vertraulichkeit der TOE schützen muss.

46 Exakte Anforderungen an die Umsetzung werden im Schutzprofil jedoch ausdrücklich nicht
47 getroffen, stattdessen wird auf die TR verwiesen:

48 *“It is essential that Processing Profiles correctly define the amount of information that must be sent*
49 *to an external entity. Exact regulations regarding the Processing Profiles [...] are beyond the scope*
50 *of this Protection Profile.” [BSI-CC-PP-0073, Application Note 2]*

51 **Klarstellung:**

52 Application Note 2 ist so zu interpretieren, dass nur solche Processing Profiles konfigurierbar
53 sein dürfen, welche die Tarifierungsanwendungsfälle nach [BSI-TR-03109-1] bzw. den dazu ver-
54 öffentlichten Errata-Dokumenten (insbesondere [TR-Errata_TAF9_10] und [TR-Errata_TAF14])
55 umsetzen. Weitere Processing Profiles sind nicht zulässig und dürfen vom SMGW nicht akzep-
56 tiert werden.

57 3 Pseudonymisierung

58 [BSI-CC-PP-0073, 6.8.2] fordert, dass das SMGW beim Versand von Daten, die weder abrech-
59 nungsrelevant noch relevant für den sicheren Betrieb des Netzes sind, die Privatsphäre des
60 Letztverbrauchers durch die Vergabe von Pseudonymen schützt:

61 „FPR_PSE.1 Pseudonymity

62 *FPR_PSE.1.1: The TSF shall ensure that [external entities in the WAN] are unable to determine the*
63 *real user name bound to [information neither relevant for billing nor for a secure operation of the*
64 *Grid sent to parties in the WAN].*

65 *FPR_PSE.1.2: The TSF shall be able to provide [aliases as defined by the Processing Profiles] ~~of the~~*
66 *~~real user name~~ for the Meter and Gateway identity to [external entities in the WAN].*

67 [...]

68 **Application Note 54:** *When the TOE submits information about the consumption or production of*
69 *a certain commodity that is not relevant for the billing process nor for a secure operation of the*
70 *Grid, there is no need that this information is sent with a direct link to the identity of the consumer.*
71 *In those cases the TOE shall replace the identity of the consumer by a pseudonymous identifier.*
72 *Please note that the identity of the consumer may not be their name but could also be a number (e.g.*
73 *consumer ID) used for billing purposes.”*

74 Das SFR konkretisiert auf diese Weise die Vorgaben aus § 52 Absatz 3 MsbG.

75 Explizit werden dabei Fälle ausgenommen, in denen die Pseudonymisierung dem eigentlichen
76 Verwendungszweck entgegensteht sowie nach §56 Absatz 1 Letztverbraucher, bei denen Netz-
77 zustandsdaten

- 78 1. „An Anlagen nach dem Erneuerbare-Energien-Gesetz und dem Kraft-Wärme-Kopplungs-
79 gesetz,
80 2. An unterbrechbaren Verbrauchseinrichtungen in Niederspannung nach §14a des Energie-
81 wirtschaftsgesetzes [und]
82 3. An Zählpunkten mit einem Jahresstromverbrauch von über 20000 Kilowattstunden“

83 erhoben werden oder nach §59 Absatz 2, Fälle in denen

- 84 1. „eine Einwilligung des Anschlussnutzers vorliegt, die den Anforderungen des § 4a des Bun-
85 desdatenschutzgesetzes genügt.“

86 **Klarstellung**

87 Durch die Formulierung als Sicherheitsanforderung ist damit Pseudonymisierung zwingend zu
88 implementieren. Im Rahmen einer CC-Evaluation wird die Umsetzung dieser Funktionalität
89 untersucht.

90 Um im Falle von TAF 10 die Pseudonymisierung beim Versand von Netzzustandsdaten – wo
91 notwendig – durchzuführen, muss diese im jeweiligen Processing Profile parametrierbar sein.

92 Da im Fall von TAF 14 nur „nicht abrechnungsrelevante Daten“ versendet werden, dabei aber
93 die Pseudonymisierung dem Verwendungszweck entgegenstünde, darf der Tarifierungsanwen-
94 dungsfall nur dann angewendet werden, wenn der betreffende Letztverbraucher dieser Ver-
95 wendung seiner Daten zugestimmt hat. Damit ist für den TAF14 eine Pseudonymisierung nicht
96 notwendig.

97 Verantwortlich für die korrekte Parametrierung ist der SMGW-Administrator. Dadurch ist das
98 SMGW in der Lage, den Sicherheitsanforderungen gerecht zu werden.

99 Wenn eine Pseudonymisierung erforderlich ist, muss auf innere Signaturen verzichtet werden.
100 Das heißt, Signaturen müssen ausschließlich außerhalb des für den berechtigten Empfänger
101 verschlüsselten CMS-Containers liegen.

102 4 Logdaten für den Letztverbraucher

103 Nach [BSI-CC-PP-0073, 6.2.3.1.1] muss das SMGW bei jedem Versand von „Meter Data“ das den
104 Versand auslösende Processing Profile sowie die versandten Werte im Logbuch des betreffen-
105 den Letztverbrauchers hinterlegen:

106 **“FAU_GEN.1/CON: Audit data generation for consumer log**

107 *FAU_GEN.1.1/CON: The TSF shall be able to generate an audit record of the following auditable*
108 *events:*

- 109 a) *Start-up and shutdown of the auditfunctions;*
- 110 b) *All auditable events for the [not specified] level of audit; and*
- 111 c) *[all audit events as listed in Table 11and [assignment:additional events or none]].*

112
113 *FAU_GEN.1.2/CON: The TSF shall record within each audit record at least the following infor-*
114 *mation:*

- 115 a) *Date and time of the event, type of event, subject identity (if applicable), and the outcome*
116 *(success or failure) of the event; and*
- 117 b) *For each audit event type, based on the auditable event definitions of the functional com-*
118 *ponents included in the PP/ST, [additional information as listed in Table 11and [assign-*
119 *ment:additional events or none]]*

120 [...]

Event	Additional Information
<i>Any change to a Processing Profile</i>	<i>The new and the old Processing Profile</i>
<i>Any submission of Meter Data to an external entity</i>	<i>The Processing Profile that lead to the submission</i> <i>The submitted values</i>
<i>Any submission of Meter Data that is not billing-relevant</i>	-
<i>Billing-relevant data</i>	-
<i>Any administrative action performed</i>	-
<i>Relevant system status information including relevant errors</i>	-

121 *Table 11: Events for consumer log”*

122 Dem SFR zufolge muss nach Tabelle 11 Zeile 2 also jeder Versand von Messwerten geloggt wer-
123 den, wobei im Logeintrag sowohl das auslösende Processing Profile, als auch die versendeten
124 Werte („additional information“) festgehalten werden.

125 **Klarstellung**

126 Für die Umsetzung von TAF 9, 10 und 14, wie in [TR-Errata_TAF9_10] und [TR-Errata_TAF14]
127 beschrieben, müssen auch Abtastraten von Zählern im Sekundenbereich möglich sein. Dabei
128 werden ausschließlich Werte erfasst, die nicht abrechnungsrelevant sind.

129 Das SFR ist auf das Sicherheitsziel O.Log gemappt, welches besagt: „*The TOE shall maintain a set*
130 *of log files as defined in [BSI-TR-03109-1] as follows: [...]*“

131 2. *A consumer log that contains information about the information flows that have been ini-*
132 *tiated to the WAN and information about the Processing Profiles causing this information*
133 *flow as well as the billing-relevant information and information about the system status*
134 *(including relevant error messages)” [BSI-CC-PP-0073, 4.1]*

135 Daher ist nach O.Log die Anweisung in Tabelle 11 des PP so zu lesen, dass nur im Falle des Ver-
136 sands von abrechnungsrelevanten Daten („*billing-relevant information*“) die versendeten Werte
137 geloggt werden müssen (Tabelle 11, Zeile 2). Der Versand von nicht abrechnungsrelevanten Da-
138 ten nach Zeile 3, beispielsweise für TAF 9, 10 und TAF 14, erfordert dies nicht.

139 Zeile 3 der Tabelle 11 („*Any submission of Meter Data that is not billing-relevant*“) wird außerdem
140 so interpretiert, dass nur solche Versendungen von nicht abrechnungsrelevanten Daten geloggt
141 werden müssen, die nicht bereits aus dem zugehörigen Processing Profile ersichtlich sind. Das
142 heißt, dass bei TAF 9, TAF 10 und TAF 14, wie in [TR-Errata_TAF9_10] und [TR-Errata_TAF14]
143 beschrieben, der Zeitpunkt der Aktivierung bzw. Deaktivierung der jeweiligen Processing Pro-
144 files im Letztverbraucherlog protokolliert werden muss. Darüber hinaus müssen bei TAF 9 und
145 TAF 10 bei Versendungen, die auf Veranlassung des SMGW-Administrator im Auftrag des be-
146 rechtigten Empfängers durchgeführt werden, die Versandzeitpunkte im Letztverbraucherlog
147 protokolliert werden. Die Möglichkeit zum Abruf der Parametrierung des Regelwerks zusam-
148 men mit den Logeinträgen ist für die Information des Letztverbrauchers ausreichend.

149 Zeile 4 der Tabelle 11 („*Billing-relevant data*“) bezieht sich wie Zeile 2 auf die Übermittlung von
150 abrechnungsrelevanten Werten und es entstehen hier keine zu Zeile 2 zusätzlichen Anforde-
151 rungen.

152 **5 Wiederholter Messwertversand**

153 Nach [BSI-CC-PP-0073, 4.1] muss das SMGW solange versuchen, Messwerte zu versenden, bis
154 der Versand entweder erfolgreich war oder eine konfigurierbare Anzahl an Versandversuchen
155 fehlgeschlagen ist:

156 „**O.Meter:** *The TOE receives or polls information about the consumption or production of different*
157 *commodities from one or multiple Meters and is responsible for handling this Meter Data.*

158 *This includes that: [...] the TOE shall store processed Meter Data if an external entity cannot be*
159 *reached and re-try to send the data until a configurable number of unsuccessful retries has been*
160 *reached.”*

161 **Klarstellung**

162 Da bei TAF 9 und 10 gemäß [TR-Errata_TAF9_10] und für TAF 14 nach [TR-Errata_TAF14] nur
163 Daten erhoben werde, die nicht abrechnungsrelevant sind, ist die Vorhaltung von alten Mess-
164 daten nicht zweckdienlich. Das PP ist an dieser Stelle dahingehend zu verstehen, dass hier ab-
165 rechnungsrelevante Daten gemeint sind. Für die TAFs 9,10 und 14 sind daher erneute Versand-
166 versuche von Netzzustandsdaten nicht zwingend erforderlich.

167 6 Communication Concealing

168 [BSI-CC-PP-0073, 6.8,1] fordert, dass das SMGW verhindert, dass durch Analyse des Datenflus-
169 ses persönliche identifizierbare Informationen gewonnen werden können.:

170 „FPR_CON.1: Communication Concealing

171 *FPR_CON.1.1: The TSF shall enforce the [Firewall SFP] in order to ensure that no personally identi-
172 fiable information(PII) can be obtained by an analysis of [assignment: characteristics of the infor-
173 mation flow that need to be concealed].*

174 *FPR_CON.1.2: The TSF shall connect to [assignment: list of external entities] in intervals as follows
175 [selection: weekly, daily, hourly, [assignment: other interval]] to conceal the data flow*

176 [...]

177 **Application Note 53:** *The interval and the list of external entities that shall be used in FPR_CON.1.2
178 highly depends on the actual application case. Therefore, the assignments in FPR_CON.1.2 are left
179 to the ST author.”*

180 [BSI-CC-PP-0073, 4.1] definiert überdies, dass diese Verschleierung gegen Analyse von Fre-
181 quenz, Last, Größe oder Fehlen jeglicher Kommunikation effektiv sein muss:

182 **“O.Conceal:** *To protect the privacy of its consumers, the TOE shall conceal the communication with
183 external entities in the WAN in order to ensure that no privacy-relevant information may be ob-
184 tained by analysing the frequency, load, size or the absence of external communication.”*

185 Klarstellung

186 Das SFR ist auch für TAF 9 und 10 gemäß [TR-Errata_TAF9_10] und TAF 14 nach [TR-Er-
187 rata_TAF14] umzusetzen, um das Sicherheitsziel zu erfüllen.

188 Im Hinblick auf den ereignisbasierten Versand von Messdaten für TAF 9, 10 und 14, der Auslöser
189 wie das Über-/Unterschreiten bestimmter Schwellwerte umfasst, können hier Maßnahmen
190 notwendig werden, die über die derzeit implementierten Verfahren hinausgehen.

191 Unter anderem besteht die Gefahr, dass nach Bekanntwerden von Schwellwerten Informatio-
192 nen über das Nutzverhalten des jeweiligen Anschlussnutzers auch durch Dritte abgeleitet wer-
193 den können. Da die den Versand auslösenden Processing Profiles vom GWA ohne Mitwirkung
194 oder Handhabe des Anschlussnutzers eingebracht werden, muss das SMGW in der Lage sein,
195 den LV effektiv vor diesem Informationsleck zu schützen.

196

197 **7 Referenzen**

- | | |
|---------------------|--|
| [BSI-CC-PP-0073] | Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, BSI. |
| [BSI-TR-03109-1] | Technische Richtlinie BSI TR-03109-1 - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0.1, BSI. |
| [TR-Errata_TAF9_10] | Errata für die BSI TR-03109-1 v1.0.1 – TAF9 und TAF10, Version 1.0, BSI. |
| [TR-Errata_TAF14] | Errata für die BSI TR-03109-1 v1.0.1 – TAF14 Hochfrequente Messwertbereitstellung für Mehrwertdienste, Version 1.0, BSI. |

198