

Stellungnahme

Technische Richtlinie BSI TR-03109-1 v1.1

bne-Stellungnahme zu den neuen BSI-Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems (TR-03109-1, Version 1.1) und Detailspezifikationen vom 30.6.2021

Berlin, 9. August 2021. Der Bundesverband Neue Energiewirtschaft e.V. (bne) begrüßt grundsätzlich die überarbeitete Technische Richtlinie (TR) des BSI. In den vorgelegten Anforderungen an die Interoperabilität der Kommunikationseinheit von Smart-Meter-Gateways (SMGW) ist die erforderliche Weiterentwicklung erkennbar und viele offene Punkte wurden konkretisiert. Nach Ansicht des bne gibt es allerdings auch Nachbesserungsbedarf bevor die TR im Ausschuss Gatewaystandardisierung zur Abstimmung gestellt wird. Im Einzelnen richtet sich die Kritik des bne gegen die Begrenzung der zu erfassenden Messgrößen in den Tarifanwendungsfällen (TAF) 9, 10 und 14, die fehlende Möglichkeit zur Wiederverwendung von Gateways nach deren Ausbau und die übertriebenen Vorgaben zur sicheren Lieferkette beim Transport der SMGW zum Kunden. Obwohl die Interoperabilität das zentrale Thema der TR ist, fehlt hierzu ein Zielbild im Dokument, es wird auch kein Weg dahin aufgezeigt. Weitere Anmerkungen des bne betreffen technische Details der in der TR beschriebenen Anforderungen.

Die überarbeitete Technische Richtlinie (TR) und die ergänzenden Detailspezifikationen präzisieren viele, bislang unklare Punkte. Der bne begrüßt daher grundsätzlich die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorlegte TR. Seitens der Entwickler bei den Gateway-Herstellern gab es positives Feedback insbesondere zu den Ausführungen zur Übermittlung von Messwertbündeln mit EN13757-3 Compact Profile beim WMBUS, zur automatischen Adresskonfiguration

an der HAN-Schnittstelle sowie zum Netzwerkdiagnoseservice. Bei anderen Punkten sieht der bne jedoch noch Änderungsbedarf und würde der vorliegenden TR-Fassung nur unter dem Vorbehalt der vorzunehmenden Änderungen zustimmen. Unsere Änderungswünsche und Kritikpunkte erläutern wir nachfolgend im Detail.

I. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Messwertverarbeitung für Tarifierung, Bilanzierung, Netzzustandsdatenerhebung

Auf Seite 89 steht zu **TAF 14**: „Das SMGW MUSS für diesen Anwendungsfall die Messgrößen in Tabelle 4.11 unterstützen. [REQ.MWV.Taf14.130] Weitere Messgrößen DARF das SMGW NICHT unterstützen. [REQ.MWV.Taf14.140]“. Diese Ausschlussregelung ist zu weitreichend. Denn hierdurch wird TAF 14 unnötig beschränkt und bleibt hinter den tatsächlichen Möglichkeiten zurück. Die Vorgabe ist zudem nicht sinnvoll. Die fehlenden Spannungswerte lassen sich zwar aus anderen Messwerten ableiten, sinnvoller wäre es jedoch, diese direkt zu messen.

Das Ziel der SMGW-Standardisierung sollte doch sein, mit den zertifizierten SMGW möglichst viele Anwendungen umsetzen zu können. Dafür müssen die Anforderungen offener gestaltet werden. Die TR ist daher dahingehend anzupassen: „Weitere Messgrößen **KANN** das SMGW unterstützen. [REQ.MWV.Taf14.140]“.

➤ Keine Begrenzung der zu erfassenden Messgrößen bei TAF 14, 9 und 10

Die gleiche Kritik gilt auch für **TAF 9** (Seite 83: „Das SMGW MUSS für diesen Anwendungsfall die Messgrößen in Tabelle 4.7 unterstützen. [REQ.MWV.Taf9.180] Weitere Messgrößen DARF das SMGW NICHT unterstützen. [REQ.MWV.Taf9.190]“) und **TAF 10** (Seite 86: „Das SMGW MUSS für diesen Anwendungsfall die Messgrößen in Tabelle 4.9 unterstützen. [REQ.MWV.Taf10.190] Weitere Messgrößen DARF das SMGW NICHT unterstützen. [REQ.MWV.Taf10.200]“). Auch hier sollte „weitere Messgrößen **DARF** das SMGW **NICHT** unterstützen“ durch „weitere Messgrößen **KANN** das SMGW unterstützen“ ersetzt werden.

Darüber hinaus wäre bei TAF 10 beispielsweise auch die **Messung der Blindleistung** von Interesse. Außerdem wäre eine Antwort auf die Frage wünschenswert, wie mit der Einbindung von (alten) modernen Messeinrichtungen umzugehen ist, die diese Messanforderungen nicht leisten können.

Lebenszyklus des SMGW

Mit Kapitel 7 widmet sich ein ganzer Abschnitt des TR-Dokuments dem Lebenszyklus von intelligenten Messsystemen und macht hierzu genaue Vorgaben. Manche davon mögen aus Sicherheitserwägungen berechtigt sein, einige Punkte sollten jedoch kritisch hinterfragt werden:

➤ Wiederverwendung statt Verschrottung von SMGW ermöglichen

Der in der TR beschriebene Prozess nach dem Ausbau des SMGW sieht einzig und allein dessen Verschrottung vor. Die Möglichkeit der Weiter- bzw. Wiederverwendung (nach einer Reparatur oder Generalüberholung) ist nicht vorgesehen. Anders als dargestellt, kann Anlass für den Ausbau des Gateways auch ein MSB-Wechsel oder der Ablauf der Eichfrist sein. Grundsätzlich ist einfach das Wegwerfen der Gateways nicht mehr zeitgemäß und keine nachhaltige Option – weder im Hinblick auf den Umgang mit Ressourcen noch mit Blick auf die Gesamtkosten. Die Wiederverwendung ist auch deshalb wichtig, da der Prozess zur Herstellung der Interoperabilität noch ziemlich am Anfang steht und eine adäquate Interoperabilität wahrscheinlich erst in mehreren Jahren erreicht wird. Die Weiterverwendung von geprüften und bereinigten SMGW muss daher möglich sein. Die TR ist entsprechend anzupassen.

➤ Zielbild zur Interoperabilität entwickeln und ergänzen

Anhand den Darlegungen zum Lebenszyklus von SMGW in der TR fällt erneut auf, dass ein Zielbild zum angestrebten Interoperabilitätsniveau in der TR fehlt. Kapitel 2.3 enthält zwar einige Hinweise des BSI, was darunter zu verstehen ist und was nicht. Aber zum einen lässt sich über diesen Standpunkt streiten (etwa, ob die Austauschbarkeit dazu gehört oder nicht) und zum anderen wird nicht klar, ob die dort dargelegte Definition das Zielniveau darstellt oder eine Weiterentwicklung geplant ist.

➤ Prozessvorgaben zur sicheren Lieferkette bei Erstauslieferung streichen

In Kapitel 7.9 werden Vorgaben zur Erstauslieferung von intelligenten Messsystemen in deren Einsatzumgebung gemacht; u.a. wird die Anforderung an Gateway-Hersteller erwähnt, eine sichere Lieferkette gemäß Common Criteria (CC) zu gewährleisten. Die sichere Lieferkette ist keine Anforderung des Messstellenbetriebsgesetzes, sondern wurde vom BSI in die CC geschrieben mit der Absicht, „die Integrität (Schutz gegen unerkannte Manipulation) und Authentizität (Schutz gegen Einbringen von gefälschten Geräten) der SMGWs auf dem kompletten Lieferweg bis zum finalen Einsatzort“¹ sicherzustellen. Die Absicht mag richtig sein, die daraus vom BSI abgeleiteten Prozessanforderungen an die sog. sichere Lieferkette sorgen für unverhältnismäßigen Aufwand bei den Herstellern und regelmäßiger Verwunderung bei den beauftragten Monteuren. Der Zugewinn an Sicherheit aus diesen Prozessvorgaben ist längst nicht mehr erkennbar. Zudem ist die Umsetzung des Prozesses nicht nur extrem aufwendig, sondern auch sehr teuer: Ein einziger Hersteller der speziellen Transportboxen bestimmt den Markt und kassiert sogar für

¹ https://www.bmwi.de/Redaktion/DE/Parlamentarische-Anfragen/2018/19-4823.pdf?__blob=publicationFile&v=4

jeden auszustellenden Freigabecode eine Gebühr. Auf der anderen Seite werden selbst Telefon-, Bank- und Kreditkarten ohne besondere Sicherheitsvorkehrungen mit der Briefpost an die Kunden versendet. Nach einer ehrlichen Kosten-Nutzen-Abwägung zur sicheren Lieferkette, kann es kaum eine andere Schlussfolgerung geben, als diesen unnötigen Prozess unverzüglich aus der CC zu streichen.

II. TR-03109-1 Detailspezifikationen

Anforderungen an Wireless M-Bus-Protokoll (Kapitel 9.2)

Der TR-Entwurf sieht hier nur den Telegramm Mode S als verpflichtend vor, während die Modi C und T lediglich optional umzusetzen sind. Die optionale Vorgabe schwächt die angestrebte Interoperabilität. Außerdem gilt Mode S inzwischen als veraltet, wird nur noch selten verwendet und für OMS auch nicht mehr empfohlen. Zum anderen ist dieser Modus auch bezüglich des Strombedarfs in den Endgeräten ungünstig. Aus diesen Gründen ist es sinnvoll, ebenfalls Mode C und T in der TR verpflichtend vorzusehen und damit das Angebot der unterschiedlichen Modi auf SMGW-Seite (stromversorgt) obligatorisch zu machen.

III. Weitere Anmerkungen

Möglicherweise ist die **Verwendung der OBIS-Kennzahlen** in der TR nicht ganz regelkonform (siehe z.B. Abschnitt 4.2.8.2.). Statt „1-0:1.8.0.255“ müsste es „1-0:1.8.0*0“ lauten; siehe dazu folgender Ausschnitt aus der EDI@Energy Codeliste der OBIS-Kennzahlen für den deutschen Energiemarkt (Stand: 17. Dezember 2019):

			OBIS - Value-Group					
			A	B	C	D	E	F
Medium	1-stellig	Elektrizität (= 1) , Gas, Wasser, Wärme...	←	←	←	←	←	←
Trennzeichen 1		- ASCII 2D	←	←	←	←	←	←
Kanal	1- oder 2-stellig	interne oder externe Kanäle, nur bei mehreren Kanälen	←	←	←	←	←	←
Trennzeichen 2		: ASCII 3A	←	←	←	←	←	←
Messgröße	1- oder 2-stellig	Wirk-, Blind-, Scheinleistung, Strom, Spannung,...	←	←	←	←	←	←
Trennzeichen 3		: ASCII 2E	←	←	←	←	←	←
Messart	1- oder 2-stellig	Maximum, aktueller Wert, Energie...	←	←	←	←	←	←
Trennzeichen 4		: ASCII 2E	←	←	←	←	←	←
Tarifstufe	1- oder 2-stellig	Tarifstufe, z.B. Total, Tarif 1, Tarif 2...	←	←	←	←	←	←
Trennzeichen 5		* ASCII 2A	←	←	←	←	←	←
Vorwertzählerstand	1- oder 2-stellig	00...99	←	←	←	←	←	←

A B C D E werden im deutschen Energiemarkt verwendet



Bundesverband Neue Energiewirtschaft (bne)
Der bne verbindet Wettbewerb, Erneuerbare und Innovation im Energiemarkt.
Seine Mitgliedsunternehmen lösen alte Grenzen auf und setzen die Kräfte der
Energiewende frei.