Bundesverband
Neue Energiewirtschaft e.V.
Hackescher Markt 4
D-10178 Berlin

Fon: +49 30 400548-0
Fax: +49 30 400548-10
mail@bne-online.de
www.bne-online.de

Stellungnahme

Technische Richtlinie BSI RC TR-03109-5

Stellungnahme des bne zur Technischen Richtlinie BSI TR-03109-5 „Kommunikationsadapter“ in der RC Version 1.0

Berlin, 13. Oktober 2023: Der bne begrüßt, dass mit dem vorliegenden Entwurf des RC1 der TR-03109-5 eine weitere Lücke bei der Umsetzung von § 14a EnWG geschlossen wird. Leider gestaltet der Entwurf die Anbindung steuerbarer Verbrauchseinrichtungen deutlich komplizierter, als es notwendig wäre.

Allgemeine Anmerkungen

Der regulatorische Rahmen gibt gemäß BNetzA-Festlegung BK6-22-300 vor, dass ab 1. Januar 2024 neu installierte privaten Ladestationen, Wärmepumpen und Speicher in ihrer Leistungsaufnahme begrenzt werden können. Die dazu notwendige Kommunikation vom Messstellenbetreiber zur Anlage muss gemäß Messstellenbetriebsgesetz über den CLS-Kanal des SMGWs abgewickelt werden. Jedes Gerät, welches diesen CLS-Kanal auf HAN-Seite terminiert, ist eine CLS-Komponente gemäß vorliegendem RC1 der TR-03109-5. Um der Steuerbarkeitsverpflichtung zu entsprechen, können die genannten Wärmepumpen, Ladestationen und Speicher entweder selbst den CLS-Kanal terminieren und somit die Funktion der CLS-Komponente einnehmen oder sie benötigen eine vorgelagerte CLS-Komponente.
Beide Optionen sind gemäß TR-03109-5 technisch aufwendig, zu hohen Kosten und mit langem Vorlauf umsetzbar. Dass eine der genannten Anlagen selbst die Funktion der CLS-Komponente

übernimmt, ist mit dem RC1 der TR-03109-5 praktisch unmöglich: Die Anlage in ihrer Gesamtheit würden den Regeln des RC1 unterworfen, da das physische Gehäuse für die Abgrenzung des Anwendungsbereichs ausschlaggebend ist. Da weiterhin praktisch jede Ladestation, Wärmepumpe oder jeder Speicher über eine Backend-Anbindung oder lokale IT-Schnittstellen zu weiteren Komponenten verfügt, müssten die zumeist für den weltweiten Vertrieb hergestellten Anlagentypen die beschleunigte Sicherheitszertifizierung (BSZ) durchlaufen – beim Inverkehrbringen, wie auch bei jedem Software-Update. Der Verzicht auf die Backend-Anbindung - und somit die BSZ - bleibt eine rein theoretische Option, weil solche Anlagen die Erwartungen der Kundinnen und Kunden nicht erfüllen würden, und in ihrer Funktionalität stark beschnitten würden.

Realistische Anforderungen an eine CLS-Komponente

Die CLS-Komponente sollte kompatibel sein mit allen am Markt verfügbaren SMGWs. Hierzu liefert der vorliegende Entwurf zusammen mit dem Testsystem des BSI einen wichtigen Beitrag.

Die CLS-Komponente muss Schnittstellen möglichst vieler aktueller und derzeit in Entwicklung befindlicher Anlagen ansprechen können, ohne dass die Anlagen dafür angepasst werden müssen. Dazu zählen ModBus/KNX, CAN, ProfiBus, aber auch WLAN, ModBus TCP, Bluetooth, ZigBee/Thread, DECT NR+.

Die jeweilige Anlage sollte sich nicht verpflichtend an der CLS-Komponente authentisieren müssen; andererseits aber sollte die CLS-Komponente für die angebotenen Schnittstellen und Protokolle das jeweils aktuelle Authentisierungsverfahren anbieten.

Die Forderung nach authentischen und integren Software-Update-Paketen für die CLS-Komponente ist sehr zu begrüßen, wie auch die Forderung nach einem Schutz vor Versions-Downgrades. Allerdings sollte die TR-5 offenlassen, wie das Update umgesetzt
wird.

Es sollte möglich sein, eine CLS-Komponente als abgeschlossenes (self-contained) Bauteil in einer anderen Anlage zu verbauen – ohne, dass dadurch die komplette Anlage in der durch ihr Gehäuse vorgegebenen Begrenzung als CLS-Komponente betrachtet wird.

Für Hersteller und Verwender der CLS-Komponente gilt die DSGVO. Für darüberhinausgehende Datenschutzanforderungen an den Kommunikationsadapter fehlt nach unserer Rechtsauffassung die gesetzliche Grundlage.

Anmerkungen im Einzelnen

Zu „1.1 Vorwort“

In Absatz 2 und Absatz 4 sollte klargestellt, dass lediglich Anforderungen an solche Komponenten im HAN getroffen werden, welche als CLS-Kommunikationsadapter (d.h. mit Nutzung der TLS-Proxy-Funktionalität des SMGW) fungieren, aber keine über die -1 hinausgehenden Anforderungen an solche Komponenten gestellt werden, welche die TLS-Proxy-Funktion nicht nutzen. Ebenso sollte in Absatz 2 und Absatz 4 klargestellt werden, dass in der Folge der Anforderungen dieser TR (siehe REQ.GEN.Schnittstellen.20) auch solche CLS-Komponenten von der Richtlinie betroffen sind, welche eine Kommunikation zu anderen HAN-Komponenten aufbauen.

Zu „1.5 Zertifizierungen“

Der letzte Absatz ist in Abhängigkeit von der Bedeutung von REQ.GEN.Schnittstellen.20 ggf. fehlleitend formuliert. Sollte REQ.GEN.Schnittstellen.20 wirklich dahingehend verstanden werden müssen, dass eine Kommunikation zu anderen Komponenten im HAN nur zulässig ist, sofern diese über „Lokale IT-Schnittstellen“ oder „Fernzugriffschnittstellen“ kommuniziert. Im Kern steckt dahinter die Frage, ob eine Zertifizierung für die CLS-Komponente erforderlich ist, wenn diese lediglich im HAN mit dem SMGW (bzw. über das SMGW) und mit anderen Komponenten im HAN kommuniziert.

Zu „2.1 Kommunikationsadapter des SMGW“

Aus unserer Sicht ist eine klarere Darstellung „weiterer Netzwerke“ notwendig, da diese aufgrund der technischen Realität auf absehbare Zeit von höchster Relevanz bleiben und auch in den kommenden Darstellungen referenziert werden.

In Absatz zwei sollte unbedingt die „Steuerungseinheit“ (bzw. „Steuerbox“) und das „EMS“ in die Liste der gewöhnlich an das SMGW bzw. an die HAN angeschlossenen Komponenten aufgenommen werden.

Zu „2.2 Systemarchitektur…“

Die Ausführungen würden von einer tabellarischen Aufbereitung der unterschiedlichen Umsetzungsvarianten und den dabei resultierenden Anforderungen profitieren. Es sollte dringend eine weitere Umsetzungsvariante aufgenommen werden, welche die Kommunikation der CLS-Komponente mit einer unmittelbar nachgelagerten Komponente im HAN umfasst, wobei diese nachgelagerte Komponente selbst aber explizit um keine TLS-Proxy-Kommunikation mit dem SMGW

abwickelt. Dies ist insofern wichtig, als dass bei nachgelagerten Komponenten explizit davon gesprochen wird, dass diese sich nicht im HAN befinden.

Zu „2.3.2 Physische Abgrenzung“

Die Trennung der Netzwerke kann auch innerhalb der CLS-Komponente durch geeigneten IT-seitigen Aufbau sichergestellt werden. Wenn Hersteller von technischen Einrichtungen diese als CLS-Komponente gemäß TR-03109-5 zertifizieren wollen, stellt eine exklusive physische Schnittstelle zur Anbindung der HAN-Schnittstelle des SMGW insbesondere bei Bestandsanlagen ein hardwareseitiges Problem dar. Um diesen, effizienten Einsatz vorhandener technischer Einrichtungen als CLS-Komponente nicht zu gefährden, ist eine Klarstellung erforderlich, dass die physische Schnittstelle der CLS-Komponente zur Anbindung an die HAN-Schnittstelle des SMGW nicht exklusiv für diesen Kanal vorgesehen ist.

Zu „2.4 Gegenstand der Konformitätsprüfung“

Dem Entwurf nach ist der Gegenstand der Konformitätsprüfung die gesamte physische CLS-Komponente, die den CLS-Kommunikationsadapter realisiert. Aus unserer Sicht ist es nicht notwendig, sowohl bei der Konformitätsprüfung nach TR als auch bei der Zertifizierung nach BSZ auf die gesamte CLS-Komponente abzustellen. Insbesondere bei der Konformitätsprüfung nach TR ist eine Beschränkung auf den CLS-Kommunikationsadapter ausreichend, wenn eine zusätzliche BSZ-Prüfung stattfindet.

Zu „2.5 Mögliche Schnittstellen von CLS-Komponenten“

Bitte um deutliche Klarstellung, dass weitere Komponenten, die nicht als CLS-Komponenten qualifizieren, auch nicht implizit über die Anforderungen dieser TR erfasst werden können bzw. Auswirkungen auf die erforderlichen Schnittstellenkategorien der CLS-Komponente haben. Dies steht in Abhängigkeit von der Bedeutung von REQ.GEN.Schnittstellen.20.

Zu „2.7.2 Anforderungen an die IT-Sicherheit“

Es ist positiv zu sehen, dass die Anforderungen lediglich an die Komponente gestellt werden, welche den CLS-Kommunikationsadapter realisiert und damit als CLS-Komponente realisiert. Es ist dagegen kritisch zu sehen, dass dabei diese Anforderungen an die gesamte physische Komponente gestellt werden und frühere Ansätze der „Software Separation“ keine weitere Berücksichtigung finden.
Darüber hinaus muss sichergestellt werden, dass die BSZ nicht bei jedem Firmware-Update neu durchlaufen werden muss, sondern nur bei solchen Firmware-Updates, welche den CLS-

Kommunikationsadapter betreffen. Ist ein CLS-Kommunikationsadapter in eine physische CLS-Komponente integriert, welche weitere Funktionalitäten aufweist, so sind häufige Firmware-Updates (z.B. monatlicher Turnus) üblich, welche die Funktion der logischen Einheit CLS-Kommunikationsadapter aber überhaupt nicht betreffen. Es ist in der Praxis nicht umsetzbar, bei jedem Firmware-Update der physischen CLS-Komponente ein BSZ-Verfahren zu durchlaufen.

Zu „2.9 Abgrenzung des Prüfgegenstands und der Schnittstellen“

Wir bitten dringend um Klarstellung, ob sich REQ.GEN.Schnittstellen.20 auf jegliche lokale Kommunikation im HAN bezieht (also auch von CLS-Komponente zu anderen Komponenten im HAN) und diese damit mit „lokalen IT-Schnittstellen“ gleichgesetzt wird, oder ob dies nicht der Fall ist und lediglich die Kommunikation zum SMGW selbst gemeint ist. Sollte ersteres der Fall sein, so wäre eine Kommunikation der CLS-Komponente zu anderen Komponenten im HAN nur zulässig, sofern die CLS-Komponente formal über „Lokale IT-Schnittstellen“ oder „Fernzugriffschnittstellen“ kommuniziert.

Zu „3.4.2.3 Anforderungen“

In Absatz 2 ist aufzuklären, ob mit der Mindestanforderung „mindestens 2 TLS-Proxy-Verbindungen“ nicht auch direkt eine Limitierung der parallelen CLS-Verbindungen einhergeht, da jede TLS-Proxy-Verbindung über das SMGW auch eine TLS-Verbindung zum SMGW selbst benötigt. Es sollte erwogen werden, die Anzahl der mindestens geforderten TLS-Proxy-Verbindungen von 2 auf 5 erhöhen. Dies ist für die praktische und interoperable Nutzbarkeit von CLS-Komponenten essenziell. Ebenfalls ist dringend informativ klarzustellen, wie viele TLS-Verbindungen und TLS-Proxy-Verbindungen ein SMGW mindestens zur Verfügung stellen muss auch in Bezug auf Anforderungen in anderen TR.

Zu „3.5.2.2 Auslöser“

Die Anforderungen zum Zeitabgleich sollten von 2 Minuten auf 15 Minuten hochgesetzt werden, sodass eine Überlastung von IT-Systemen aufgrund eines durch einen großflächigen Stromausfall induzierten Neustarts der Komponenten besser vermieden kann.
Aus gleichen Gründen sollte die Anforderung um den Aspekt der Randomisierung der Anfragen innerhalb des maximalen Zeitraums ergänzen.

Zu „3.5.2.3 Anforderungen“

Es ist nicht nachvollziehbar, wieso eine Begrenzung auf 31.12.2049 erfolgt. Diese Begrenzung ist gefährlich, da sich bereits in der Vergangenheit immer wieder gezeigt hat, dass bewährte Komponenten deutlich über 25 Jahre Nutzungszeit erreichen können.

Zu „5.3 Sicherheitsfunktionalität“

In der Praxis muss auch die Möglichkeit bestehen, existierende Steuerungsprotokolle im LAN, die keine TLS-Verschlüsselung unterstützen, anzusteuern. Es ist nicht zielführend Hersteller zur Umstellung einer gesamten Produktpalette zu zwingen, die Kosten verursachen und Ressourcen binden, jedoch lediglich den deutschen Markt betreffen. Daher empfehlen wir, bei Kryptographie (Punkt 4) auf das Wort „sollte“ verzichten und dieses durch ein „kann“ zu ersetzen.
Weiter bitten wir um Klarstellung, was bei Punkt 6 mit „keine kritischen Informationen“ gemeint ist. Hier ist eine eindeutige Definition notwendig.