bitkom

Stellungnahme zur technischen BSI TR-03109-5

Auf einen Blick

Technische Richtlinie BSI TR-03109-5

Ausgangslage

Die Technische Richtlinie BSI-TR-03109 umfasst die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Einzelkomponenten in einem intelligenten Messsystem erfüllen müssen. Die BSI TR-03109-5 regelt insbesondere die Anforderungen an weitere Systemeinheiten des intelligenten Messsystems und soll die sichere kommunikative Anbindung von technischen Einrichtungen an das Smart-Meter-Gateway ermöglichen.

Bitkom-Bewertung

Wir begrüßen, dass die Bundesregierung und das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun die technische BSI TR-03109-5 für die sichere Anbindung und Fernsteuerbarkeit von steuerbaren Einrichtungen am Netzanschlusspunkt vorgelegt hat und im Ausschuss Gateway Standardisierung beschließen will. Damit kommt eine standardisierte und interoperable Umsetzung für Anwendungen im CLS nun endlich in greifbare Nähe. Es gilt aber auch: Nur mit eindeutiger, verständlicher und praktikabler Standardisierung haben die Marktakteure die nötige Sicherheit, um den Rollout voranzutreiben.

Wir halten den Entwurf grundsätzlich für geeignet, die Standardisierung der Kommunikationsadapter herzustellen. Wir sehen es allerdings kritisch, dass der Entwurf eine Sicherheitszertifizierung der gesamten physischen Einheit fordert, welche den CLS-Kommunikationsadapter realisiert. Dies wird in der praktischen Umsetzung eine Realisierung mit separaten FNN-Steuerboxen bedeuten. Der frühere Ansatz der „Software Separation“ sollte weiterhin berücksichtigt werden damit der Zertifizierungsaufwand für viele Hersteller und Anbieter von anderen Komponenten, wie v.a. Energiemanagementsystemen (EMS), die ihre Software regelmäßig (bspw. monatlich) mit Funktionsupdates aktualisieren, in einem sinnvoll zu leistenden niedrigen Rahmen bleibt. Im Endeffekt werden damit marktübliche und praktikable Umsetzungsoptionen für EMS mit direkter Kommunikation zum SMGW, insbesondere zur Umsetzung von §14a EnWG mit EMS, massiv erschwert und de facto nicht realisierbar. Gleiches gilt für CLS-Lösungen, die kundenindividuelle Mehrwertsoftware sicher in die Smart-Meter-PKI integrieren wollen. Deshalb müssen weitere Vereinfachungen für Softwareanpassungen in Kommunikationsadapter vorgesehen werden.

Im Folgenden möchten wir einige Vorschläge und Anmerkungen zu einzelnen, technischen Aspekten und Passagen der technischen Richtlinie darlegen, welche insbesondere einer eindeutigen, verständlichen und praktikablen Umsetzung der TR zugutekommen sollen.

Inhalt

1 Stellungnahme zur technischen BSI TR-03109-5

Zu 1.1: Vorwort

In Absatz 2 und/oder Absatz 4 sollte klargestellt werden, 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.

Außerdem sollte klargestellt werden, dass in der Folge der Anforderungen dieser TR (siehe Kommentar zu 2.9) auch solche CLS-Komponenten von der Richtlinie betroffen sind (bzw. sein können, siehe Kommentar zu 2.9), welche eine Kommunikation zu anderen HAN-Komponenten aufbauen.

Der Begriff „HAN-Kommunikationsszenario (HKS)“ sollte als Abkürzung bereits im Vorwort eingeführt werden, da die Abkürzung HKS im Verlauf der TR häufige Verwendung findet.

Zu 1.5: Zertifizierungen

Der letzte Absatz ist in Abhängigkeit von der Bedeutung von REQ.GEN.Schnittstellen.20 (siehe Kommentar zu 2.9) 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, stellt das eine starke Einschränkung für EMS dar, sollte dies eindeutig so formuliert und angeführt werden.

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, nicht aber mit anderen Komponenten außerhalb des HAN.

Zu 2.1: Kommunikationsadapter des SMGW

Die Darstellung zur Aufnahme „weiterer Netzwerke“ sollte überarbeitet werden, da diese aufgrund der technischen Realität auf absehbare Zeit von höchster Relevanz bleiben und auch in den kommenden Darstellungen referenziert wird. Möglicherweise sollte hier über die Aufnahme des Begriffs „AB-LAN“ (LAN des Anlagenbetreibers) diskutiert 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 für CLS-Kommunikationsadapter

Die Ausführungen würden von einer tabellarischen Aufbereitung der unterschiedlichen Umsetzungsvarianten und den dabei resultierenden Anforderungen profitieren.

Es sollte 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 2.5: Mögliche Schnittstellen von CLS-Komponenten

Es sollte explizit klargestellt werden, 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 (siehe Kommentar zu 2.9).

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 kritisch zu sehen, dass dabei diese Anforderungen an die gesamte physische Komponente gestellt werden und frühere Ansätze der „Software Separation“ keine weitere Berücksichtigung finden. Stattdessen sollten „Software Separation“ als geeignetes Mittel aufgenommen werden, um den Zertifizierungsgegenstand für die BSZ-Zertifizierung einzugrenzen, zumal nicht ersichtlich ist, dass das Sicherheitsniveau insgesamt steigt, wenn in Konsequenz entscheidende Funktionen auf einer separaten Hardware außerhalb der CLS Komponente vorgenommen werden.

Zu 2.9: Abgrenzung des Prüfgegenstands und der Schnittstellen

Die Formulierung zu REQ.GEN.Schnittstellen.30 ist missverständlich, da sie impliziert, dass eine CLS-Komponente mehrere Schnittstellen zum HAN haben kann, die dann aber wiederum alle die gleiche IP haben müssen. Das wiederum wäre in einem Netzwerk aber nicht zulässig.

Es sollte explizit klargestellt werden, 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.

Die zentrale Information der Fußnote 5 sollte auch in den Haupttext, z.B. unter „1.4 Anwendungsbereich der TR“, eingearbeitet werden. Zudem sollte möglichst auch auf die Implikationen der Feststellung in Fußnote 5 eingegangen werden.

Zu 3.2.2.3: Anforderungen

Wenn CLS_HAN_TLS_PUB immer der gleiche Schlüssel sein muss, der in CLS_HAN_TLS_CRT steht, dann ist es nicht notwendig diesen separat zu übergeben. Er kann in der Schnittstelle entfallen.

Eine Zertifikatsprüfung mit CLS_HAN_TLS_PUB kann durch eine direkte Prüfung des Self-Signed Zertifikates ersetzt werden. Da die Schlüssel ja sowieso übereinstimmen müssen, ist diese Prüfung gleichwertig.

Auf jeden Fall fehlt die Prüfung im CLS-Kommunikationsadapter, ob CLS_HAN_TLS_PRV zu CLS_HAN_TLS_CRT passt. Sollte dies durch eine fehlerhafte Implementierung im SMGW nicht der Fall sein, wäre der CLS-Kommunikationsadapter nämlich nicht mehr in der Lage, TLS-Handshakes mit dem SMGW durchzuführen.

Zu 3.2.5.2: Auslöser

Der ICS.FA.PinSmgwCertificate.10 bedarf einer Schärfung.

Es muss klar reglementiert werden, wie und unter welchen Bedingungen ein Akteur diese FA auslösen darf. Wenn dazu z.B. eine lokale Schnittstelle wie USB verwendet werden kann, so muss trotz allem irgendeine Art Authentifizierung stattfinden, damit ein Angreifer nicht einfach ein eigenes TLS-Zertifikat unterschieben kann.

Es muss sichergestellt werden, dass nur eine vertrauenswürdige Rolle den Pinning Vorgang einleiten kann. Generell müssen hier Sicherheitsmechanismen implementiert werden, die verhindern, dass unerlaubte TLS-Zertifikate den Weg in den CLS-Kommunikationsadapter finden.

Zu 3.3.1.1: Beschreibung

Hier ist nicht klar, ob FA.RestoreDefaults auch aktiv ein Firmware-Update auslösen muss. Die Formulierung „Auslieferungszustand … mit neuester Firmware“ kann so interpretiert werden, dass ein Restore nur mit neuester Firmware erlaubt ist. In dem Fall muss also entweder das Update automatisch stattfinden oder der CLS-Kommunikationsadapter prüfen, ob die neueste Firmware installiert ist und ggf. FA.RestoreDefaults ablehnen muss, falls dies nicht so ist.

Zu 3.4.2.2: Auslöser

Der CLS-Kommunikationsadapter MUSS entweder FA.RequestProxyCh ODER FA.AcceptProxyCh implementieren. Ansonsten kann keine Verbindung aufgebaut werden.

Zu 3.4.2.3 Anforderungen

Absatz 2 sollte informativ bezüglich der Mindestanzahl der TLS-Verbindungen und TLS-Proxy-Verbindungen eines SMGWs auf die TR-03109-1 verweisen. Diese Information ist für die Interoperabilität essenziell. Im Sinne der praktischen, interoperablen Nutzung sollte überlegt werden die Anzahl der parallelen TLS-Proxy Verbindungen von 2 auf 5 zu erhöhen.

Zu 3.5.2: FA.DoTimeSync

Wenn ein CLS-Kommunikationsadapter HKS.TLSPROXY.CLI, HKS.TLSPROXY.SOCKSCLI oder HKS.TLSPROXY.SRV nutzen muss, weil das SMGW keinen NTP-Server bereit stellt oder dieser nicht funktioniert, so impliziert dies folgendes:

1. Jede Zeitsynchronisation erfordert eine CLS-Verbindung im WAN. Hier ist bereits aus Erfahrung mit der Zeitsynchronisation der SMGWs zu erwähnen, dass dies zu einer ungewollten DoS Attacke auf den Zeitserver führen kann. In diesem Fall wäre es dann allerdings keine DoS Attacke auf den Gateway Administrator, sondern auf den CLS-Kanal des aEMT, über den die NTP Server Funktionalität abgebildet wird.
2. Da CLS im WAN generell kein Protokoll vorgibt, müsste der CLS-Endpunkt im aEMT entweder eine Weiche implementieren, die erkennt, ob es sich bei dem Traffic um eine NTP-Anfrage handelt. Oder es müssen alternativ im aEMT mehrere CLS-Endpunkte angeboten werden, die dedizierte Aufgaben wie z.B. eben NTP übernehmen. Letzteres wiederum bedeutet, dass im SMGW verschiedene CLS-Profile hinterlegt werden müssen und das SMGW vermutlich selbst auch verschiedene CLS-Endpunkte im HAN bereitstellen muss. Dies wiederum führt so weiteren Konfigurationsprofilen im CLS-Kommunikationsadapter, der dann mehrere CLS-Endpunkte zum SMGW verwalten muss.

Zu 3.5.2.2 Auslöser

Die Anforderungen zum Zeitabgleich sollte von 2 Minuten auf 60 Minuten hochgesetzt werden, sodass eine Überlastung von IT-Systemen aufgrund eines durch einen großflächigen Stromausfall induzierten Neustarts der Komponenten besser vermieden werden kann.

Aus selbigen Gründen sollte unbedingt die Anforderung um den Aspekt der Randomisierung der Anfragen innerhalb des maximalen Zeitraums ergänzt werden.

Zu 3.5.2.3: Anforderungen

Die Begrenzung auf 31.12.2049 erschließt sich uns nicht. Diese Begrenzung ist gefährlich, da sich bereits in der Vergangenheit immer wieder gezeigt hat, dass bewährte

Komponenten deutlich über 25 Jahre Nutzungszeit erreichen können. Es ist nicht erkennbar, wieso dieser Zeitraum gewählt wurde.

Der Hersteller hat hier keine andere Möglichkeit als zu deklarieren, dass er es NICHT gewährleisten kann, eine geringere Abweichung als 9 Sekunden zu haben.

Dies liegt daran, dass der Hersteller

- keinen Einfluss auf die Verfügbarkeit des Zeitservers und dessen Erreichbarkeit hat
- zwischen Produktion und Einbau des CLS-Kommunikationsadapters Monate oder Jahre vergehen können, die eine Zeitsynchronisation unmöglich machen

ICS.FA.DoTimeSync.10 ist daher dahingehend zu präzisieren, dass sich das ICS ausschließlich auf die Abweichung der Systemzeit des CLS-Kommunikationsadapters zwischen zwei Synchronisationsintervallen handelt. Im Zweifel, sollte in Betracht gezogen werden, die ICS.FA.DoTimeSync.10 ersatzlos zu streichen.

Zu 3.5.2.4: Implementierungshinweise

In Anbetracht der bereits oben erwähnten möglichen DoS Attacken sollte ein CLS-Kommunikationsadapter bestenfalls einmal stündlich seine Zeit synchronisieren.

Zu 4.4.5.1 Beschreibung

Hierzu stellt sich uns die Frage, ob die BSI TR-03109-1-WAN TLS-Client Funktionalität mit ServerNameIndication RC1-20.10.2017 finalisiert wird.

Zu 5.3: Sicherheitsfunktionalität

Bei den Services, Punkt 6 sollte eindeutig klargestellt werden, was mit „keine kritischen Informationen“ gemeint ist. Dazu findet sich bisher keine genauere Definition.

Bei Kryptographie, Punkt 4 sollte auf das Wort „sollte“ verzichtet und dieses in eine „soll“ geändert werden.

Eindeutige Bezeichner der Kriterien würden zur Praktikabilität der TR helfen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Felix Janssen | Referent für Energy & Smart Grids
T 030 27576-271 | f.janssen@bitkom.org

Verantwortliches Bitkom-Gremium
AK Smart Grids