Datensicherheit bei der Funkübertragung Ultraschallzähler Qalcosonic W1

Einleitung

Im Bereich der Übertragung von Daten aus Verbrauchsmessgeräten wie Wasser-, Wärme-, Gas- und Stromzählern gibt es verschiedene Ansatzpunkte dies vorzunehmen. Neben kabelgebundenen Lösungen verbreitet sich die Funkübertragung immer mehr.

Da die gesetzlichen Grundlagen der vier Medien in vielen Fällen nicht gleich sind, sind auch die Lösungen grundsätzlich unterschiedlich zu bewerten.

Bereich	Wasser und Wärme	Strom und Gas
Zuständigkeit	Bundeskartellamt/Landesbehörde	Bundesnetzagentur/Landesregulierung
Grundlage	VABWasserV/Heizkostenverordnung etc.	EnWG/MsbG
Messwesen	Wasser ist nicht liberalisiert Wärme durch die FFVAV (Teil-)liberalisiert	Liberalisiert

Als weiteren **Hinweis** darf aufgeführt werden, dass man sich bei den verschiedenen Lösungen natürlich an die vorhandenen Vorgaben halten muss. Hier ist jedoch zu unterscheiden, ob es sich um ein Gesetz, eine Verordnung, eine Richtlinie oder nur um eine Information handelt und ob diese jeweils für alle oder nur für einzelne Medien gültig sind.

Aufgrund der Vielfalt der Lösungen und der dadurch großen Komplexität behandelt dieses Dokument nur die Funkübertragung wie sie bei Wasserzählern meist zum Einsatz kommt. Teilweise werden ergänzende Hinweise aus den Bereichen der anderen Medien mit aufgenommen, die aber sicher nicht vollständig sein werden und nur zum besseren Verständnis dienen sollen.

Bei Wasserzählern kommen meist zwei Funklösungen zum Einsatz:

1. wMBus (wireless MBus)
    a. für die „lokale/mobile“ Auslesung im walk-by/drive-by Verfahren
    b. für die „lokale/stationäre“ Anbindung an ein Smart Meter Gateway (SMGW)
2. LoRaWAN
    a. für die „entfernte/stationäre“ Übertragung an LoRaWAN Gateways

Ein Wasserzähler mit einer Funkoption kann ein mechanischer Wasserzähler mit einem aufgebauten oder extern angeschlossenen Funkmodul sein aber auch ein elektronischer oder hybrider Wasserzähler mit elektronischem Zählwerk.

Der DVGW hat im September 2022 für den Bereich elektronischer oder hybrider Wasserzähler die **DVGW-Information Wasser Nr. 114 „Elektronische Wasserzähler“** veröffentlicht. Bei der Erstellung haben wir als Ernst Heitland GmbH & Co.KG neben anderen Herstellern und Anwendern mitgearbeitet und unser Wissen und unsere Erfahrungen eingebracht.
Es ist anzumerken, dass es sich hier lediglich um eine Informationsschrift handelt, die das allgemeine Wissen bündelt und für Anwender bereitstellt. Es handelt sich nicht um eine techn. Richtlinie oder gar um eine Verordnung oder um ein Gesetz und somit sind die Inhalte nicht rechtsverbindlich, wenn nicht auf rechtsverbindliche Quellen verwiesen wird.

Tel.: 0212 710 55 Fax.: 0212 765 43
info@heitland-gmbh.de www.heitland-gmbh.de

Datensicherheit bei der Funkübertragung Ultraschallzähler Qalcosonic W1

Grundlagen/Begriffsdefinitionen

Ein „Smart Meter Gateway“ (SMGW) ist laut Definition des BSI ein Teil eines „intelligenten Messsystems“ (iMsys). Der andere Teil ist die „moderne Messeinrichtung“ (mME). Ein iMsys kann das SMGW und die mME in einem Gerät vereinen oder es können auch zwei separate Geräte vorhanden sein.

Ein iMsys ist i. d. R. ein digitaler Stromzähler oder ein Gaszähler mit Kommunikationsadapter. **Ein elektronischer Wasserzähler fällt auf jeden Fall NICHT unter die Definition eines iMsys/mME.** Der Hintergrund dazu ist einfach und simpel.

Definition: Quelle: https://www.bundesnetzagentur.de/SharedDocs/A_Z_Glossar/M/ModerneMesseinrichtung.html?nn=706202
Eine **moderne Messeinrichtung (mME)** ist ein Messgerät (z. B. digitaler Stromzähler), der

I. den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt **(detaillierte Verbrauchsdarstellung**)
II. über ein Smart-Meter-Gateway sicher in ein Kommunikationsnetz eingebunden werden kann
III. nicht fernausgelesen werden kann
IV. keine Zählerstände sendet (d.h. eine manuelle Ablesung durch den Messstellenbetreiber oder den Kunden ist weiterhin notwendig)

Auf den ersten Blick wird man sicher vermuten, dass ein elektronischer Wasserzähler auch unter die Definition eines mME fällt, aber beim genaueren Hinsehen zeigt sich:

- Zu I. trifft nicht zu: Ein Wasserzähler misst Wasser und keine Energie
- Zu II. trifft bedingt zu: Nur wenn wie aufgeführt der Wasserzähler mit OMS-Mode 7 seine Daten überträgt
- Zu III. trifft nicht zu: Elektronische Wasserzähler sind i.d.R. fernauslesbar
- Zu IV. trifft nicht zu: Ein el. Wasserzähler sendet seinen Zählerstand

Allein der Punkt I wäre ausreichend um ein Wasserzähler NICHT als mME zu bezeichnen.

Da ein el. Wasserzähler somit klar KEIN iMsys und auch KEIN mME ist findet die Richtlinie BSI TR-03116 (Kryptographische Vorgaben für Projekte der Bundesregierung) keinerlei Anwendung.

Dieser Sachverhalt ist von immenser Bedeutung für alle die Funkwasserzähler z. B. über ein LoRaWAN Netz fernauslesen wollen.

Bei Wasserzählern ist IMMER der Zählerstand AUF dem Zähler (LCD-Anzeige) der für die Abrechnung relevante Wert und NICHT der per Funk oder anderweitig übertragene und somit „nachgebildete“ Zählerstand.
Im Gegensatz zu einem iMsys wird der Zählerstand im Wasserzähler gebildet und übertragen. Das trifft im Sinne auch dann zu, wenn Wasserzähler und Funkmodul voneinander getrennt (clip-on/extern) sind. Im iMsys hingegen wird der Zählerstand zwar auch im Zähler (z. B. Stromzähler) gebildet aber laut Definition durch das SMGW übertragen welches den Anforderungen der TR-03116 entsprechen muss.

Daher sind bei Wasserzählern die sehr sicheren, aber auch sehr aufwendigen Verschlüsselungsverfahren nach TR-03116 nicht anzuwenden.

Datensicherheit bei der Funkübertragung Ultraschallzähler Qalcosonic W1

Diese sind insgesamt weit über den Zielvorgaben der Funkübertragung bei Wasserzählern angesiedelt und überflüssig.
Die Funkübertragung von Zählerständen von Wasserzählern dient ausschließlich als Unterstützung und Vereinfachung der Ablesung/Abrechnung sowie weiteren Anwendungen wie z. B. der Wasserverlustanalyse und internen Bilanzierungen.

Das bedeutet nicht, dass bei einem entfernten/stationären Funksystem (z. B. LoRaWAN) keine Verschlüsslung notwendig ist. Es reicht hier aber völlig aus sich an die Empfehlungen der TR-02102-1 zu halten. Darin sind weit mehr Verfahren benannt als in der strengen TR-03116. In der TR-02102-1 wird zudem in der Einleitung darauf hingewiesen, dass:

[… Es wird dabei jedoch ausdrücklich kein Anspruch auf Vollständigkeit erhoben, das heißt nicht aufgeführte Verfahren werden vom BSI nicht zwangsläufig als unsicher beurteilt. Umgekehrt ist allerdings auch der Schluss falsch, dass kryptographische Systeme, die als Grundkomponenten nur in der vorliegenden Technischen Richtlinie empfohlene Verfahren verwenden, automatisch sicher sind. ...]

wMBus (wireless MBus)

Für die Funkübertragung mittels wMBus gibt es ausreichend Dokumentationen, die von der OMS Group bereitgestellt werden und hier nicht weiter behandelt werden müssen.

Eine sichere Datenübertragung kann hier rein symmetrisch nach **Stand der Technik** erfolgen. Die technische Richtline (TR-02102-1) vom Bundesministerium für Informationstechnologie (BSI) beschreibt hier die Einzelheiten und gibt für die kryptographischen Verfahren entsprechende Empfehlungen.

Klarer Konsens besteht dahingehend, dass die **Funkübertragung gemäß OMS 4.0 Security Profile B (EN 13757-7 Mode 7)** das sich wiederum an die BSI TR-03116-3 anlehnt, hier eingesetzt werden kann und dem Stand der Technik entspricht – speziell im Hinblick auf die Anbindung an SMGWs.

- „Mode 7“ (Security Profile B) ist **verpflichtend** für Zähler, die Ihre Daten an ein SMGW senden.
- „Mode 5“ (Security Profile A) ist für die mobile Auslesung ausreichend aber nicht für die Kommunikation mit SMGWs zugelassen.

Wir empfehlen daher auch bei der mobilen Zählerfernauslesung den Mode 7 zu verwenden. Eine evtl. zukünftige Veränderung der Zählerfernauslesung im Rahmen des Rollouts der SMGWs ist dann einfach vorzunehmen.

Profil	Encryption/Verschlüsselung	Key/Schlüssel
Security Profile A	AES-128 CBC (ENC-Mode 5)	128 Bit Static Symmetric Key
Security Profile B	AES-128 CBC (ENC-Mode 7)	128 Bit Dynamic Symmetric Key (abgeleitet von KDF)

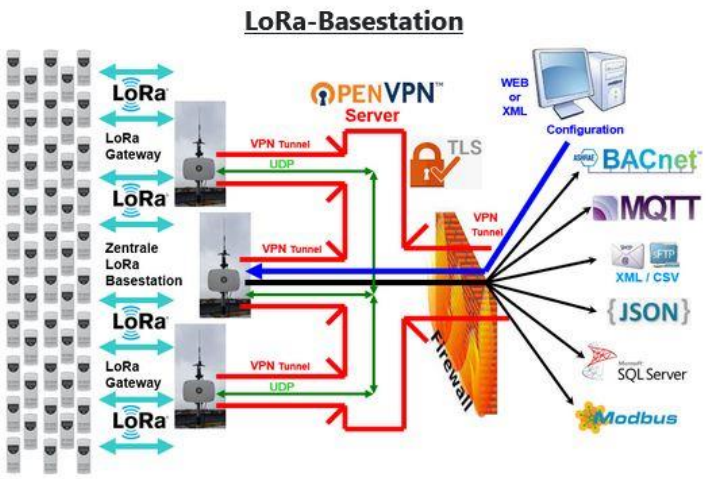
Die Zähler der Baureihe Qalcosonic halten diese Vorgaben zu 100% ein und verschlüsseln und senden die Daten gemäß den o. g. Anforderungen. **Der Ultraschallwasserzähler Qalcosonic W1 wird im Standard immer mit Mode 7 ausgeliefert und ist DVGW zertifiziert (OMS Nr. OG-4467DM0682).**

Datensicherheit bei der Funkübertragung Ultraschallzähler Qalcosonic W1

LoRa/LoRaWAN

LoRaWAN ist eines der wenigen IoT-Protokolle, das **Ende-zu-Ende-Verschlüsselung** sicherstellt.

In einigen anderen Funknetzen sind die Nachrichten nur über Funk verschlüsselt und werden ab dem Gateway/Basestation des Providers unverschlüsselt übertragen. Dies führt dazu, dass der Anwender sich selbst um eine zusätzliche Verschlüsselungsebene kümmern muss (meist wird dies über eine Art VPN oder Anwendungs-Schichtverschlüsselung wie TLS realisiert).



Quelle: Ing. Büro Lertes

Eine zusätzliche TLS- oder VPN-Verschlüsselung ab dem Zähler eignet sich nicht für LoRaWAN, da sie einen erhöhten Energieverbrauch, Komplexität und zusätzliche Kosten verursacht.
Gerade bei täglicher oder mehrfach täglicher Übertragung der Daten sind bei batteriebetriebenen Zählern dann nur sehr kurze Batterielebensdauern zu realisieren.

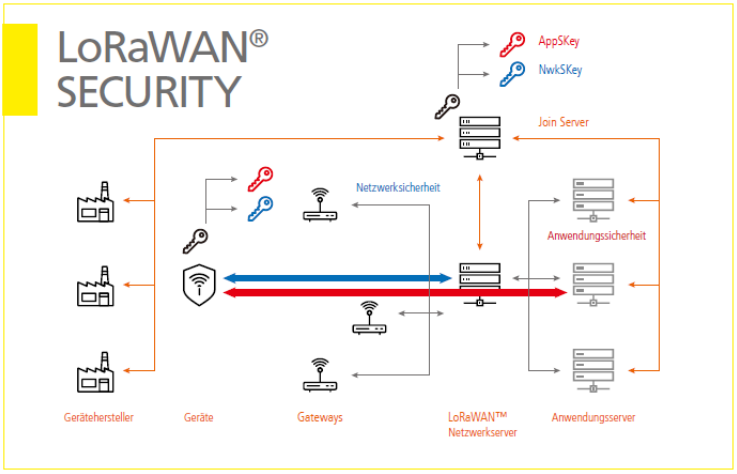
Die LoRaWAN Sicherheitsmechanismen basieren auf den bewährten und standardisierten kryptographischen AES-Algorithmen. Diese Algorithmen werden seit vielen Jahren von der kryptographischen Gemeinschaft analysiert und sind NIST zugelassen. Sie gelten allgemein als beste Sicherheitspraxis für batteriebetriebene Geräte.

LoRaWAN verwendet das kryptographische AES-Verfahren in Kombination mit mehreren Betriebsarten: CMAC2 für Integritätsschutz und CTR3 für Verschlüsselung. Jedes LoRaWAN-Gerät ist mit einem eindeutigen 128-Bit-AESSchlüssel (AppKey genannt) und einer global eindeutigen Kennung (EUI-64-basierte DevEUI) personalisiert, die beide während der Geräteauthentifizierung verwendet werden.

Auch in der **DVGW Information Wasser Nr. 114** werden unter Punkt 6.5 (Seite 35+36) verschiedene Kommunikationslösungen wie LoRaWAN aufgeführt. LoRaWAN arbeitet wie andere Systeme auch mit einer AES128-bit Verschlüsselung. Ab dem Gateway/Basisstation werden weitere Verschlüsselungen wie z. B. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 oder andere empfohlen.

Datensicherheit bei der Funkübertragung Ultraschallzähler Qalcosonic W1

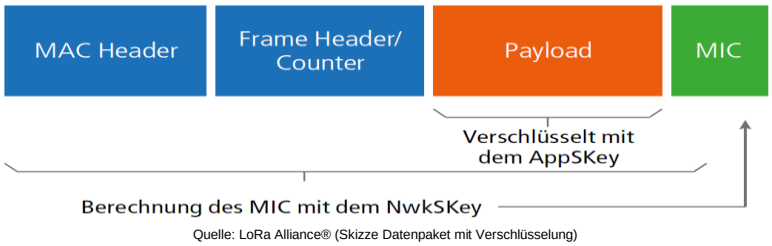
LoRaWAN verwendet das standardisierte AES-CTR[1] Verfahren, das wie andere AES-Verfahren (z.B. CBC5)[2] die XOR-Verknüpfung nutzt. Dies verstärkt die AES-Verschlüsselung, da für jeden Datenblock ein einmaliger Schlüssel verwendet werden muss.



Quelle: LoRa Alliance® (End to End Verschlüsselung)

Der komplette Datenverkehr von LoRaWAN wird mit zwei Sitzungsschlüsseln geschützt. Jedes Nutzdatenpaket (Payload) wird über AES-CTR verschlüsselt und um eine Nachrichtennummer (Frame Counter) sowie einen „Message Integrity Code“ (MIC) ergänzt.

Der MIC wird mit AES-CMAC berechnet, um eine Manipulation der Daten auszuschließen.



Quelle: LoRa Alliance® (Skizze Datenpaket mit Verschlüsselung)

Das LoRaWAN grundsätzlich als sicher eingestuft werden kann zeigt auch die Zusammenarbeit der LoRa Alliance® mit der OMS-Group. Beide arbeiten derzeit an einem Projekt, das die OMS-Datenformate über das LoRaWAN Netzwerk übertragen kann.

Die Zähler der Baureihe Qalcosonic halten diese Vorgaben zu 100% ein und verschlüsseln und senden die Daten gemäß den o. g. Anforderungen. **Der Ultraschallwasserzähler Qalcosonic W1 ist durch die LoRa Alliance® zertifiziert.**

Zusätzlich zu der o. g. AES128bit Verschlüsselung kann bei den Zählern der Qalcosonic Baureihe noch eine separate Verschlüsselung für die Payload aktiviert werden. **Diese optionale Verschlüsselung arbeitet gemäß OMS Security Profile A (Mode 5)** und bietet gegenüber anderen LoRa Slaves somit noch eine erhöhte Sicherheit gegen das Abhören und Entschlüsseln von Daten.