



Gegebenheiten beim Einsatz von Funkwasserzählern im privaten Umfeld

Einleitung

Aufgrund der Entwicklung immer kleinerer und leistungsfähigerer elektronischer Komponenten und neuer Verfahren zur Informationsübertragung haben seit Anfang der 1990er Jahre die Möglichkeiten zur mobilen Kommunikation und zur drahtlosen Übermittlung von Daten stark zugenommen. Neben neuen professionellen Funkdiensten und dem Mobilfunk, die größere Gebiete abdecken und nahezu flächendeckend verfügbar sind, gibt es mittlerweile eine Vielzahl an Geräten für eine klein- und kleinräumige drahtlose Kommunikation und Datenübertragung, die zunehmend auch im privaten Umfeld eingesetzt werden.

Auch wenn die Anwendungen sehr vielfältig, die eingesetzten Techniken im Detail sehr unterschiedlich und die technischen Standards und Herstellerspezifikationen nahezu unüberschaubar sind, so haben sie doch eine Reihe gemeinsamer Merkmale.

Die Übertragung von Sprache und Daten erfolgt per Funk. Das bedeutet zum einen, dass die ausgesandten Signale mit einem entsprechenden Empfänger auch von anderen Personen als den Adressaten aufgefangen und abgehört werden können, wenn sie nicht hinreichend verschlüsselt sind.

Funkübertragung bedeutet auch, dass von den Geräten elektromagnetische Felder abgestrahlt werden, denen die Nutzer und Personen in der Nachbarschaft ausgesetzt sind. Die Sendeleistungen der meisten im Haushalt betriebenen Geräte sind im Vergleich mit Radio-, Fernseh- und Mobilfunksendern sehr niedrig.

Wie stark einzelne Anlagen oder Geräte zur Exposition einer Person mit Funkfeldern beitragen, hängt von einer ganzen Reihe von Faktoren ab.

Die wichtigsten sind:

1. Die Sendeleistung
2. Die Sendehäufigkeit/Sendedauer
3. Der Abstand des Senders zur Person
4. Die Ausbreitungsbedingungen bezogen auf den Installationsort

Rechtliche Grundlage

In der Europäischen Union gilt die EU-Richtlinie 2014/53/EU. Diese verweist auf Grenzwerte, die in der Empfehlung des Rates der Europäischen Union (1999/519/EC) zur „Begrenzung der Exposition der Bevölkerung gegenüber elektromagnetischen Feldern (0 Hz bis 300 GHz)“ festgelegt wurden. Diese Werte stützen sich wiederum auf Empfehlungen der Strahlenschutzkommission und der Internationalen Kommission zum Schutz vor nichtionisierender Strahlung (ICNIRP). Auch die in Deutschland gültige „Verordnung über elektromagnetische Felder“ (26. BImSchV) des deutschen Bundesamtes für Strahlenschutz (BfS) orientiert sich an diesen Werten.



Gegebenheiten beim Einsatz von Funkwasserzählern im privaten Umfeld

Zu 1) Die Sendeleistung

Die o.g. Verordnung und die darin gesetzlich festgesetzten Grenzwerte gelten nur für gewerblich genutzte ortsfeste Anlagen mit einer Sendeleistung von mehr als 10 Watt (10.000mW). Für Anlagen mit geringerer Sendeleistung, mobile Sender sowie für privat betriebene Anlagen und Geräte gibt es bisher keine gesetzlichen Grenzwerte.

Die Qalcosonic W1 Ultraschallwasserzähler senden mit einer Leistung von kleiner 10 Milliwatt. (Siehe Auszug aus Testbericht No.:07112019_001 Etteplan EMV Prüfservice)

4.3 Test results – Free Space – EIRP

Channel	Frequency [MHz]	VERTICAL EIRP [dBm]	HORIZONTAL EIRP [dBm]	TOTAL EIRP [dBm]	Direction of maximum Radiation Azimuth / Elevation [deg]
Low Channel	863.1MHz	8.38	8.13	8.83	45.0 / 143.4
Default Channel	868.3MHz	9.23	9.06	9.68	45.0 / 143.4
High Channel	869.525MHz	9.31	9.28	9.79	45.0 / 143.4

Eckwerte Umrechnung: $8,13\text{dBm} = 6,5\text{mW} + 9,79\text{dBm} = 9,528\text{mW}$

- WLAN Router senden mit ca. 100mW
- DECT Schnurlostelefone senden mit 250mW
- Mobiltelefone senden mit ca. 1.000mW bis ca. 2.000mW (je nach Netz)
- Fernseher senden mit ca. 5.000.000.000 mW

Zu 2) Die Sendehäufigkeit/ Sendedauer

Für die Funkübertragung von Zählerdaten gelten internationale Regeln. Nach diesen darf ein Zähler erst nach dem 1.000fachen der Zeit, die eine Übertragung dauert, erneut senden.

Die Qalcosonic W1 Ultraschallwasserzähler senden in der Standardeinstellung nur alle 16s und das auch nur zwischen 6Uhr bis 18Uhr (Montags-Freitags). Eine Funkübertragung dauert ca. 15ms beim Langtelegramm und ca. 4 ms beim Kurztelegramm (Standard)

Zu Nachtzeiten und am Wochenende findet keine Funkübertragung statt.

Mit diesen Angaben ergibt das eine max. Sendedauer pro Tag von ca. 40,5s (Langtelegramm) und von ca. 10,8s beim Kurztelegramm.

- Schnurlostelefone, Mobiltelefone oder WLAN-Router, die selbst im Standby-Modus mit deutlich größerer Leistung senden, wirken dagegen mehrere Stunden am Tag auf den Menschen ein und das meist rund um die Uhr.



Gegebenheiten beim Einsatz von Funkwasserzählern im privaten Umfeld

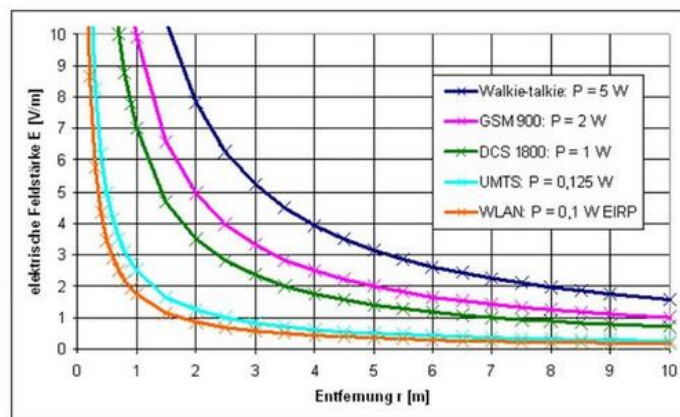
Zu 3) Der Abstand des Senders zur Person

Die Stärke elektromagnetischer Felder nimmt mit zunehmender Entfernung zur Quelle rapide ab. So beträgt die sogenannte Dämpfung selbst im freien Raum schon in einem Meter Entfernung ca. 31 Dezibel (dB). Bereits 3 dB bedeuten eine Halbierung der Sendeleistung.

Die Qalcosonic W1 Ultraschallwasserzähler sind wie alle Wasserzähler im Hausanschluss/Keller oder nahe der Hauseinführung eingebaut und befinden sich somit immer in einem größeren Abstand zu den Bewohnern der Wohnung/des Hauses.

Geräte:

TETRA: bis 10 W
 GSM 900: bis 2 W
 DCS 1800: bis 1 W
 DECT: 250 mW
 UMTS: 125 mW
 WLAN Devices: 100 mW
 Bluetooth: meist 1 – 2,5 mW



Zu 4) Die Ausbreitungsbedingungen bezogen auf den Installationsort

Die Installation der Funkwasserzähler im Hausanschlussraum/Keller führt dazu, dass das Funksignal durch Wände und Decken sendet. Diese Hindernisse im Übertragungsweg führen dazu, dass die Dämpfung (siehe auch Punkt zu 3.) deutlich größer ist als im freien Raum was die Sendeleistung die beim Menschen ankommt nochmals um ein vielfaches reduziert wird.

Im Gegensatz dazu werden Mobil- und Schnurlostelefone vom Nutzer in aller Regel direkt ans Ohr gehalten.

Zusammenfassung

Aufgrund der oben genannten Fakten ist davon auszugehen, dass der Einsatz von Funkwasserzähler zu keiner gesundheitlichen oder sonstigen Beeinträchtigung von Mensch und Tier führt.

Vor diesem Hintergrund bleibt noch zu erwähnen, dass durch die RICHTLINIE (EU) 2018/2002 DES EUROPÄISCHEN PARLAMENTS UND DES RATES bezüglich der Energieeffizienz vorsieht, dass ab 25. Oktober 2020 nur noch fernauslesbare Zähler und Heizkostenverteiler eingebaut werden dürfen, sofern das technisch und wirtschaftlich sinnvoll und möglich ist. Da es hier um Energieeinsparung geht, betrifft dies in erster Linie die Wohnungswirtschaft. Es ist abzuwarten, wann ähnliche Anforderungen an die Wasserversorgungswirtschaft gestellt werden.

Die Verwendung von Funkwasserzählern in der Wasserversorgung hat aber schon heute sehr viele Vorteile. Kosteneinsparungen bei den Versorgern und somit auch bei den Endverbrauchern werden heute schon realisiert.



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.



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 Verschlüsselung 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 Richtlinie (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)

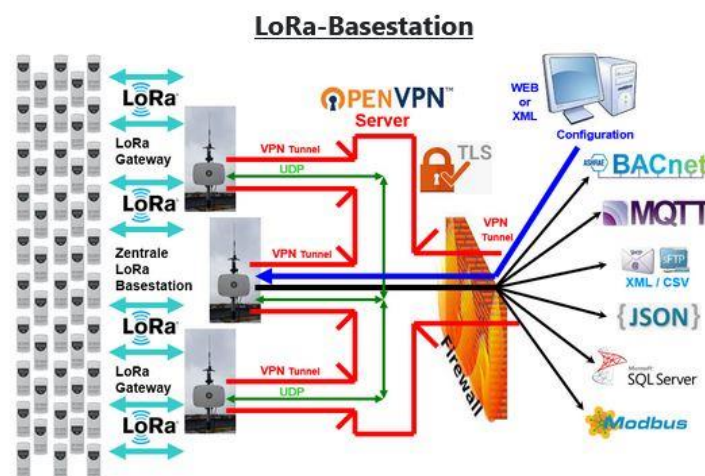
Die Zähler der Baureihe Qalcosonic halten diese Vorgaben zu 100% ein und verschlüsseln und senden die Daten gemäß den o. g. Anforderungen. **Der Ultraschallwasserzähler Qalcosonic W1 wird im Standard immer mit Mode 7 ausgeliefert und ist DVGW zertifiziert (OMS Nr. OG-4467DM0682).**

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.

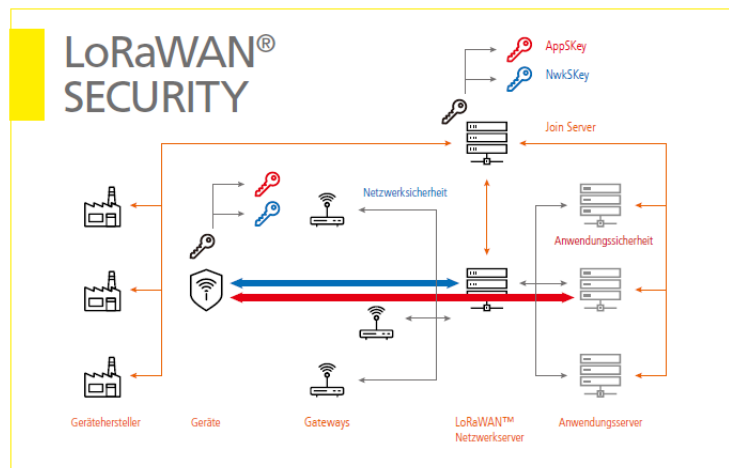
LoRaWAN verwendet das kryptographische AES-Verfahren in Kombination mit mehreren Betriebsarten: CMAC2 für Integritätsschutz und CTR3 für Verschlüsselung. Jedes LoRaWAN-Gerät ist mit einem eindeutigen 128-Bit-AESSchlüssel (AppKey genannt) und einer global eindeutigen Kennung (EUI-64-basierte DevEUI) personalisiert,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

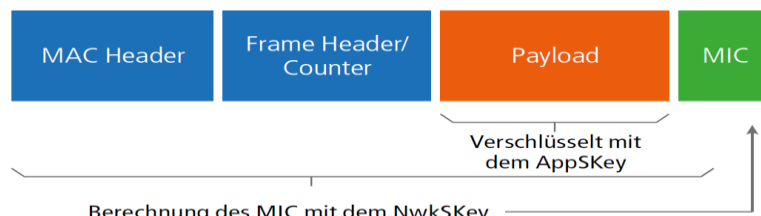
LoRaWAN verwendet das standardisierte AES-CTR⁽¹⁾ Verfahren, das wie andere AES-Verfahren (z.B. CBC5)⁽²⁾ die XOR-Verknüpfung nutzt. Dies verstärkt die AES-Verschlüsselung, da für jeden Datenblock ein einmaliger Schlüssel verwendet werden muss.



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.



Ultraschallzähler Qalcosonic Baureihe Datenverschlüsselung

Datenverschlüsselung ist ein wichtiges Thema zum Schutz vor Zugriff von Dritten mit der Absicht die Daten zu manipulieren. Aus diesem Grund gibt es verschiedene Maßnahmen, die in bei der Übertragung von Zählerdaten eingesetzt werden können.

Von der OMS Group wurden bereits in der **Spezifikation (wMBus)** Generation 1 entsprechende Festlegungen definiert, die Datenübertragungen per Funk sicher macht.

Man spricht hier von Security Profil A, B, C wobei die Security Profile A und B mit dem bekannten AES-128 Verschlüsselungscode arbeiten und das Security Profile C eine sehr aufwendige TLS-Verschlüsselung nutzt, die zudem einen sehr hohen Energieverbrauch hat.

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)
Security Profile C	TLS 1.2 (ENC-Mode 13)	256 Bit Elliptic Curve Key (384 Bit optional) for TLS and 128 Bit Dynamic Symmetric Key (abgeleitet von) for CMAC

- **Security Profile A (Mode 5)** kommt im Allgemeinen bei der mobilen Auslesung zum Einsatz und ist der Standard in Europa.
- **Security Profile B (Mode 7)** wird verwendet, wenn die Kommunikation über ein SMGW erfolgen soll. Hier sind aus dem Bereich Strom und Gas weitaus höhere Anforderungen vom BSI gestellt als bei Wasser und Wärme. Der Mode 7 kann aber auch bei mobiler Auslesung genutzt werden, sofern die nachgeschalteten Empfänger und die Auslesesoftware die Daten entsprechend entschlüsseln kann. Bei älteren Systemen kann es zu Problemen kommen.
- **Security Profile C (Mode 13)** wird i. d. R. nur bei Kommunikation im Internet verwendet sowie bei bidirektionalen Verbindungen, die bei Wasser- und Wärmezählern nicht zum Einsatz kommen.

Bei der **Ultraschallzählerbaureihe Qalcosonic W1/F1 (Wasser) und E3/E4 (Wärme)** stehen für die Übertragung von Daten über wMBus beide Datenverschlüsselungen als Option zur Verfügung. Security Profile A (Mode 5) und Security Profile B (Mode 7).

- Als Standard werden die W1 Zähler immer **mit Security Profile B (Mode 7)** ausgeliefert.
- Als Standard werden die F1/E3/E4 Zähler immer **mit Security Profile A (Mode 5)** ausgeliefert.

Ein **LoRaWAN Netzwerk** verwendet eine etwas andere Systematik. Hier wird bei der ersten Verbindung (Join Prozess) ein individueller „Zählerschlüssel“ (LoRa APP Key) ausgetauscht. Nur wenn dieser im Gateway vorliegt, kann mit der Datenübertragung begonnen werden. Danach werden die Daten in zwei Ebenen verschlüsselt: ein einheitlicher Netzschlüssel (NwksKey - AES 128) für die Netzebene und ein weiterer Netzschlüssel (AppSKey - AES 128) für die Applikationsebene (höchstmögliche Verschlüsselung im Embedded Bereich).

Der NwksKey wird für die Interaktion zwischen dem Datenknoten (Gateway) und dem Netzwerk genutzt und überprüft die Gültigkeit einer Nachricht. Der AppSKey wird für die Kodierung und Dekodierung der Payloads (Teil der Nachricht ohne Metadaten) genutzt. Beide Schlüssel sind einmalig je Gerät und Session. Durch diese Architektur gehört LoRaWAN zu den sichersten Netztechnologien, die es momentan im Funkbereich gibt.

Bei der **Ultraschallzählerbaureihe Qalcosonic W1/F1 (Wasser) und E3/E4 (Wärme)** steht als Option neben den bei LoRaWAN vorhandenen Verschlüsselungen **eine zusätzliche Verschlüsselung nach dem Muster von OMS wMBus Security Profile A (Mode 5)** zur Verfügung. Hier wird die Payload (das Datenprotokoll) zusätzlich mit AES-128 CBC (ENC-Mode 5) einem 128 Bit Static Symmetric Key verschlüsselt und kann somit nur gelesen werden, wenn der AES-Schlüssel bekannt ist.

- Als Standard werden die Zähler immer **ohne zusätzlichem Security Profile B (Mode 5)** ausgeliefert

Da nahezu alle verfügbaren LoRaWAN Slaves diese zusätzliche Mode 5 Verschlüsselung nicht bieten, bedeutet das i. d. R. einen geringen Programmieraufwand auf der Empfängerseite (Gateway/Server) welchen die meisten Softwareanbieter noch nicht umgesetzt haben.