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 Softwarenanbieter noch nicht umgesetzt haben.