STADTWERKE SCHWAZ

Technische Beschreibung
Kundenschnittstelle Stadtwerke Schwaz Smart Meter

Disclaimer:
Diese technische Beschreibung gilt für die von den Stadtwerken Schwaz eingesetzten Smart Meter der Hersteller Kaifa und Honeywell.

Einleitung
Die Kommunikation über die Kundenschnittstelle ist nach dem Stand der Technik mit einem individuellen, kundenbezogenen Schlüssel abgesichert, sodass Unberechtigten der Zugriff auf die Daten verwehrt wird. Außerdem ist die Schnittstelle standardmäßig deaktiviert.

Die Kundenschnittstelle kann über das Kundenportal der Stadtwerke Schwaz aktiviert werden. Im Anschluss wird Ihnen Ihr kundenindividueller Schlüssel zugesandt.

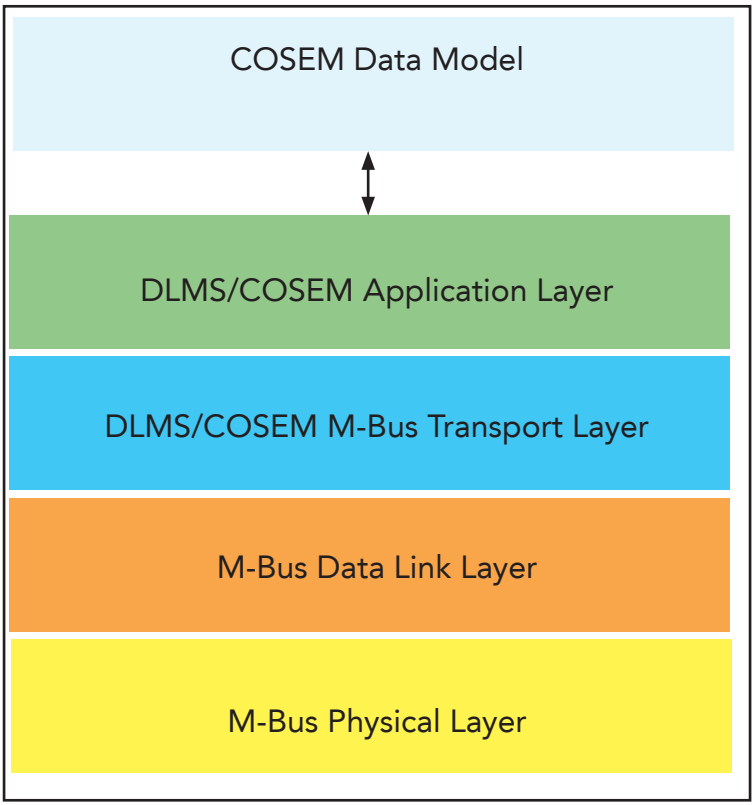
Bezüglich Ver- und Entschlüsselung der Daten sind folgende Informationen maßgeblich:

- Die Verschlüsselung findet in der Applikationsschicht statt (nicht in der Transportschicht).
- Verwendeter Sicherheitsstandard: DLMS/COSEM Security Suite 1
- Verschlüsselungsalgorithmus: AES-GCM (Advanced Encryption Standard - Galois/Counter Mode)

Stadtwerke Schwaz GmbH
Hermine-Berghofer-Straße 31, 6130 Schwaz
Tel.05242 6970, info@stadtwerkeschwaz.at

Datenübertragung und Protokollstack

Die technische Datenübertragung basiert auf einem Protokollstack auf Basis von M-Bus auf den unteren Protokollschichten in Kombination mit einer DLMS/COSEM Applikationsschicht. Darüber werden die als COSEM-Objekte codierten Nutzdaten in verschlüsselter Form übertragen.



Zusätzliche Informationen:

Protokollschicht	Detailbeschreibung zu finden in (Spezifikation/Standard/Norm)
COSEM Data Model	DLMS/COSEM Spezifikation (Blue Book) bzw. IEC 62056-6-1, IEC 62056-6-2
DLMS/COSEM Application Layer	DLMS/COSEM Spezifikation (Green Book, Kapitel 9) bzw. IEC 62056-5-3
DLMS/COSEM M-Bus Transport Layer	EN 13757-3 (M-Bus Transport Layer) und Green Book 10.5.4.6 (M-Bus wrapper)
M-Bus Data Link Layer	EN 13757-2
M-Bus Physical Layer	EN 13757-2

M-Bus Physical Layer:

Anschluss:	RJ 12 Modular Jack 6P6C
Konfiguration:	Wired M-Bus Master
Baud-Rate:	2.400
Übertragungs-parameter:	1 Startbit, 8 Datenbits, 1 Paritätsbit (gerade Parität), 1 Stoppbit
Kom.-Richtung:	Push only
Push-Intervall:	5 Sek.

Pin-Belegung:

Pin-Nr.	Belegung
1	nicht verwendet
2	nicht verwendet
3	MBUS1 (+)
4	MBUS2 (-)
5	nicht verwendet
6	nicht verwendet

Stromversorgung:
über M-Bus, max. 4 M-Bus-Loads mit insgesamt 6 mA und 32 V

M-Bus Data Link Layer & Transport Layer:

Logische Frame-Struktur

Zur leichteren Interpretation der über die physikalische Schnittstelle übertragenen bzw. empfangenen Byte-Sequenzen ist der Aufbau der Nachrich-ten, die logische Frame-Struktur, in der nachfolgenden Abbildung dargestellt. Mit diesen Informationen kann die Entschlüsselung und Dekodierung der Nutzdaten nachvollzogen bzw. durchgeführt werden.

M-Bus Data Link Layer	Start Character 68h L Field L Field Start Character 68h C Field A Field
DLMS/COSEM M-Bus Transport Layer	CI Field STSAP DTSAP
DLMS/COSEM Application Layer	Data (Encrypted DLMS Payload)
M-Bus Data Link Layer	Checksum Stop Character 16h

Feld	Protokoll-schicht	Beschreibung	Länge [bytes]	statisch	Wert [hexadezimal]
Start Character	Data Link Layer	Beginn des M-Bus Frames	1	ja	68h
L Field	Data Link Layer	Frame-Länge	1	nein	Anzahl an bytes zwischen 2. Start Character und Check-sum-Feld (= 2 + Transport Layer Length + Application Layer Length)
C Field	Data Link Layer	Control-Feld (Daten-flussrichtung, Frametyp etc.)	1	nein	53h/73h (SND_UD, SEND UserData von Master zu Slaves)
A Field	Data Link Layer	Adress-Feld (Empfänger)	1	ja	FFh (Broadcast-Adresse)
CI Field	Transport Layer	Control-Information-Feld (Struktur der nachfolgenden Transport- und Applikationsschicht-daten, Details siehe unten)	1	nein	00h-1Fh
STSAP	Transport Layer	Source Transport Ser-vice Access Point	1	ja	01h (Management Logical Device ID 1 des Zählers)
DTSAP	Transport Layer	Destination Transport Service Access Point	1	ja	67h (Consumer Information Push Client ID 103)
Data	Application Layer	Verschlüssel-te Nutzda-ten (DLMS, Details siehe unten)	max. 250	nein	
Che-cksum	Data Link Layer	Prüfsumme zur Fehlererkennung	1	nein	Arithmetische Summe der bytes zwischen 2. Start Charac-ter und Checksum-Feld ohne Berücksichtigung etwaiger Überträge
Stop Charakter	Data Link Layer	Ende des M-Bus Frames	1	ja	16h

Wie in der zuvor angeführten Tabelle beschrieben, können in einem einzelnen M-Bus Frame maximal 250 bytes an (DLMS-)Nutzdaten transportiert werden. Größere DLMS-Nachrichten müssen daher vor dem Versand in mehrere Teile (<=250 bytes) zerlegt werden (Segmentierung) und in sepa-raten M-Bus Frames verschickt werden. Der Empfänger muss die verschiedenen Teile aus den M-Bus Frames extrahieren und wieder zu einer einzelnen DLMS-Nachricht zusammenfügen (Reassemblierung).

Gesteuert wird dieser Prozess über das Control-Information-Feld.

Control-Information-Feld:

b7	b6	b5	b4	b3	b2	b1	b0
0	0	0	FIN	Sequence number			

- Bits 7, 6 und 5 gleich 0 zeigen an, dass kein separater M-Bus Datenheader präsent ist.
- Bit 4 (FIN) gleich 0 zeigt an, dass Segmentierung aktiv ist, es sich aber nicht um das letzte übertragene Segment handelt.
- Bit 4 (FIN) gleich 1 markiert das letzte Segment bzw. das einzige Segment bei inaktiver Segmentierung.
- Bits 3 bis 0 repräsentieren die jeweilige Segmentnummer.

Beispiel:
Für eine DLMS-Nachricht <=250 bytes ist CI=0x10. Bei einer DLMS-Nachricht, die in Form von 2 Segmenten übertragen werden muss, ist CI=0x00 für das 1. Segment und CI=0x11 für das 2. Segment

DLMS/COSEM Application Layer

Struktur der verschlüsselten Nutzdaten (Encrypted DLMS Payload), Aufbau der DLMS-Nachricht

DLMS/COSEM Application Layer	Ciphering Service
System Title Length	Security Control Byte
	System Title
	Length
	Frame Counter
	Security Control Byte
	Frame Counter
	Encrypted Payload

Feld	Protokoll-schicht	Beschreibung	Länge [bytes]	statisch	Wert [hexadezimal]
Ciphering Service	Application Layer	Kennung des Ver-schlüsse-lungsmechanis-mus	1	ja	DBh (general-glo-ciphe-ring)
System Title Length	Application Layer	Länge des nachfolgenden System Title in bytes	1	ja	08h
System Title	Application Layer	Eindeutige ID des Zählers (Zeichenkette)	8	ja	individuell je Zähler
Length	Application Layer	Nachrichten-länge (Security Control Byte, Frame Coun-ter, Encrypted Pay-load)	variabel	nein	Anzahl an bytes nach dem Length Feld (= 5 + Encrypted Payload Length); codiert als 1 byte für Nachrichten-länge <=127, andernfalls als 2 bytes mit Präfix 82h; z.B., 820109h für Nachrichtenlänge = 0109h = 265
Security Control Byte	Application Layer	Security Control Byte - Ein-stellung von Sicherheitspara-metern	1	ja	21h (Bits 3 bis 0: Se-curity_Suite_Id; Bit 4: “A” subfield: indicates that authentication is applied; Bit 5: “E” subfield: indicates that encryption is applied; Bit 6: Key_Set subfield: 0 = Unicast, 1 = Broadcast; Bit 7: Indicates the use of compression)
Frame Counter	Application Layer	Nachrichten-zähler	4	nein	
Encrypted Payload	Application Layer	Verschlüsselte Nutzdaten	variabel	nein	

Bezüglich Ver- und Entschlüsselung der Daten sind folgende Informationen maßgeblich:

- Die Verschlüsselung findet in der Applikationsschicht statt (nicht in der Transportschicht).
- Verwendeter Sicherheitsstandard: DLMS/COSEM Security Suite 1
- Verschlüsselungsalgorithmus: AES-GCM (Advanced Encryption Standard - Galois/Counter Mode)
- Schlüssellänge: 128 Bits
- Initialisierungsvektor (IV): 96 bits, IV = System Title + Frame Counter (Verkettung von System Title und Frame Counter)

COSEM-Datenmodell:

OBIS-Code	Attribut
0-0:1.0.0.255,1	Clock Attribute 1 - OBIS code
0-0:1.0.0.255,2	Clock attribute 2 - Datum und Uhrzeit
0-0:96.1.0.255	Zählernummer des Netzbetreibers
0-0:42.0.0.255	COSEM logical device name
1-0:32.7.0.255	Spannung L1 (V)
1-0:52.7.0.255	Spannung L2 (V)*
1-0:72.7.0.255	Spannung L3 (V)*
1-0:31.7.0.255	Strom L1 (A)
1-0:51.7.0.255	Strom L2 (A)*
1-0:71.7.0.255	Strom L3 (A)*
1-0:1.7.0.255	Wirkleistung Bezug +P (W)
1-0:2.7.0.255	Wirkleistung Lieferung -P (W)
1-0:1.8.0.255	Wirkenergie Bezug +A (Wh)
1-0:2.8.0.255	Wirkenergie Lieferung -A (Wh)
1-0:3.8.0.255	Blindleistung Bezug +R (Wh)
1-0:4.8.0.255	Blindleistung Lieferung -R (Wh)

* Werte werden ausschließlich bei Drehstrom-Zählern ausgegeben