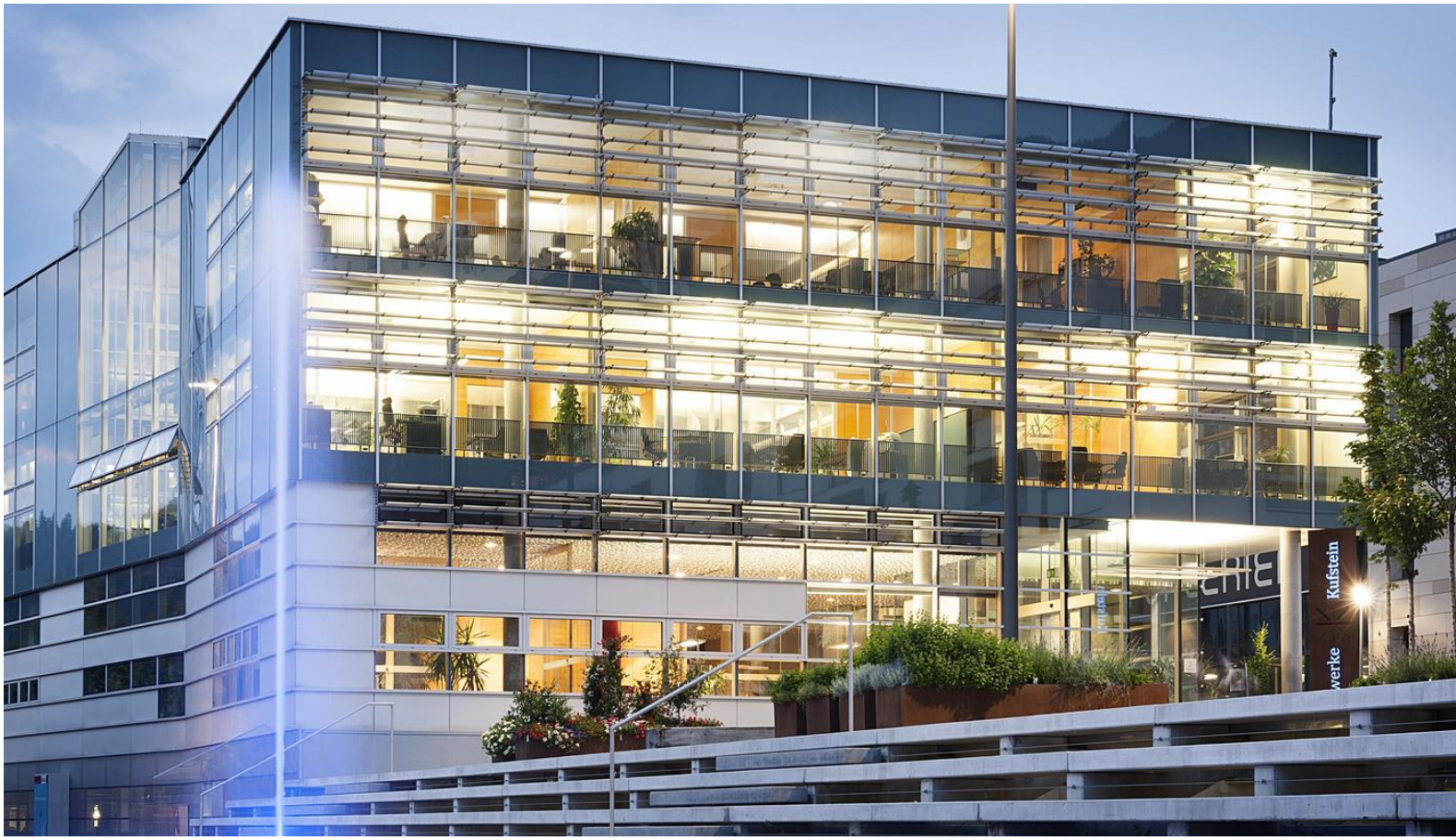
Stadtwerke Kufstein



Strom- Kundenschnittstelle Smart Meter

STADTWERKE KUFSTEIN

Die neuen, elektronischen Stromzähler sind mit einer Kundenschnittstelle ausgestattet. Über diese Kundenschnittstelle haben Sie die Möglichkeit, direkt die persönlichen Stromverbrauchswerte abzulesen.

Die Kundenschnittstelle ist standardmäßig deaktiviert und kann durch die jeweilige Kundin bzw. den jeweiligen Kunden selbst im Webportal aktiviert werden. Im Anschluss wird ein kundenindividueller Schlüssel übermittelt.

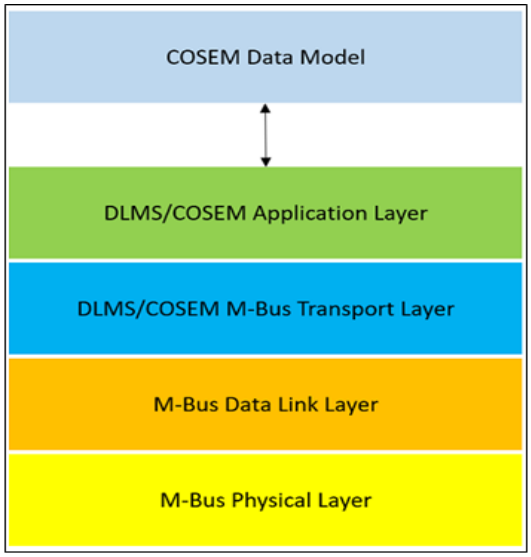
Wichtig: Wir sind als Verteilnetzbetreiber ausschließlich für den Strom- und Datenfluss zum Stromzähler und für den Stromzähler selbst verantwortlich. Für die Smart Meter Adapter und damit betriebene Programme, wie zum Beispiel Energiemonitoring-Systeme oder Smart Home-Produkte, ist der/die Kund:in selbst verantwortlich.

1. Inhalt

2. 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.



3. COSEM DATENMODELL

OBIS-Code	Attribut
0-0:1.0.0.255,1	Clock Attribute 1
0-0:1.0.0.255,2	Clock attribute 2
0-0:96.1.0.255	Zählernummer
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	Blindenergie Bezug +R (varh)
1-0:4.8.0.255	Blindenergie Lieferung -R (varh)

* Werte werden ausschließlich bei Drehstrom-Zählern ausgegeben

Zusätzliche Informationen können dem Kapitel 10.5 des DLMS/COSEM Green Book bzw. dem IDIS package 2 entnommen werden.

Nachfolgende Kapitel sind wesentlich:

- DLMS/COSEM Green Book
  - 10.5.3.4.2 MBUS-DATA service primitives
  - 10.5.3.4.3 MBUS-DATA protocol specification
  - 10.5.4 Identification and addressing scheme
    - 10.5.4.4 Link Layer Address for M-Bus broadcast
    - 10.5.4.5 Transport layer address
    - 10.5.4.6 Application addressing extension – M-Bus wrapper
- IDIS package 2
  - 6.11.3 Security on the Consumer Information Interface
  - 6.11.4 CIP System Title an Error Handling

4. DLMS/COSEM APPLICATION LAYER

Struktur der verschlüsselten Nutzdaten (Encrypted DLMS Payload), Aufbau der DLMSNachricht:

Feld	Protokoll-schicht	Beschreibung	Länge [bytes]	statisch	Wert [hexadezimal]
Ciphering Service	Application Layer	Kennung des Ver- schlüsselungsmechanismus	1	ja	DBh (general-glo-ciphering)
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	Nachrichtenlänge (Security Control Byte, Frame Counter, Encrypted Payload)	variabel	nein	Anzahl an bytes nach dem Length Feld (= 5 + Encrypted Payload Length); codiert als 1 byte für Nachrichtenlänge <=127, andernfalls als 2 bytes mit Präfix 82h; z.B., 820109h für Nachrichtenlänge = 0109h = 265
Security Control Byte	Application Layer	Security Control Byte - Einstellung von Sicherheitsparametern	1	ja	21h (Bits 3 bis 0: Security_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	Nachrichtenzähler	4	nein	
Encrypted Payload	Application Layer	Verschlüsselte Nutzdaten	variabel	nein	

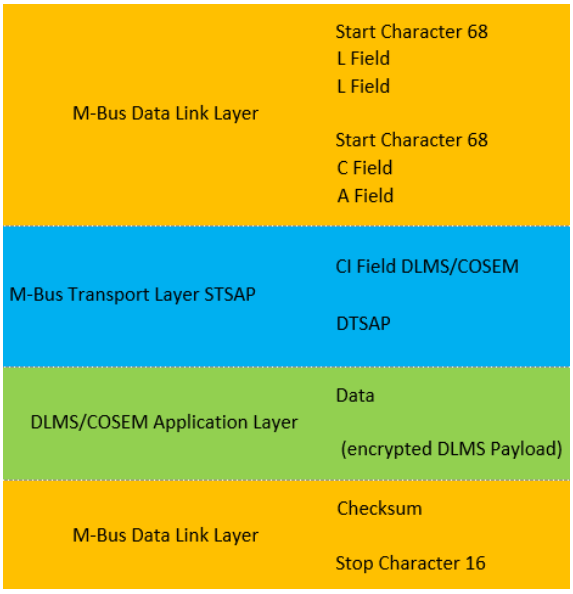
Bezüglich Ver- und Entschlüsselung der Daten sind folgende Informationen maßgeblich:

- 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)

5. 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 Nachrichten, die logische Framestruktur, in der nachfolgenden Abbildung dargestellt. Mit diesen Informationen können die Entschlüsselung und Dekodierung der Nutzdaten nachvollzogen bzw. durchgeführt werden



Feld	Protokoll-schicht	Beschreibung	Länge [bytes]	statisch	Wert [hexadezimal]
Start Character	Data Link Layer	Beginn des M-Bus Frames	1	ja	68
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 (Datenflussrichtung, 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 Applikationsschichtdaten, Details siehe unten)	1	nein	00h - 1Fh
STSAP	Transport Layer	Source Transport Service 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	Verschlüsselte Nutzdaten (DLMS, Details siehe unten)	max. 250	nein	
Checksum	Data Link Layer	Prüfsumme zur Fehlererkennung	1	nein	Arithmetische Summe der bytes zwischen 2. Start Character und Checksumfeld ohne Berücksichtigung etwaiger Überträge
Stop Character	Data Link Layer	Ende des M-Bus Frames	1	ja	16

Wie in der zuvor angeführten Tabelle beschrieben, können in einem einzelnen M-Bus

Frame maximal 250 bytes an (DLMS-)Nutzdaten transportiert werden. Größere DLMSNachrichten 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-InformationFeld:

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 repräsentiert 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.

6. M-BUS PHYSICAL LAYER

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

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

- Stromversorgung: Über M-Bus, 4 M-Bus-Loads mit insgesamt 6mA und 32V
- Protokoll Version: DLMS / COSEM, IDIS CII

7. SECURITY STANDARD

- Security Suite: Security Suite 1
- Security Profil: AES128-CBC, Security profile B laut OMS Standard Verschlüsselung:
- Key: Global Unicast Encryption Key
- Authentication: CMAC (8 Byte trunc)(MAC-Mode AT=5)