Open Metering System Technical Report 08 OMS over mioty

Version 1.0.1 / 2023-05-25
RELEASE

© Open Metering System Group e.V., 2023

Document History

- V 0.0.1: Initial template
- V 0.0.2: Input to chapter 1, 2, 3 for meeting #3
- V 0.0.3: Consolidation before meeting #4
  - Addition of abbreviations to glossary of terms
  - Addition of chapter 4.1
- V 0.0.4: Consolidation before meeting #5
  - Chapter 2.3 changed
  - Addition of chapter 4.2
  - Addition of chapter 4.3
- V 0.0.5: Editing in meeting #5
  - Chapter 1.1 changed
  - Chapter 4.1: headlines for subchapters added
  - Chapter 4.1: subchapters changed
  - Chapter 4.2.2 changed
- V 0.0.6: Consolidation before meeting #6
  - Chapter 3.3 changed
- V 0.0.7: Consolidation before meeting #7
  - Tables 3 and 5 changed
  - Figure 1 changed
  - Chapter 2.3 changed
  - Chapter 4.2.4 changed
- V 0.0.8: Editing in meeting #7
  - Chapter 2.3 changed
  - Chapter 4.1.3 changed
  - Chapter 4.2.2 changed
  - Chapter 4.2.4 changed
- V 0.0.9: Editing in meeting #8
  - Chapter 4.1.3 changed
- V 0.0.10: Editing in meeting #9
  - Chapter 4.2.3 changed
  - Chapter 4.2.4 changed
- V 0.0.11: Copyright remark added to front page
- V 0.0.12: Tables 3 and 5 aligned to OMS-S2 bit format
- V 0.0.13: Consolidation after meeting #11
  - Tables 3 and 5 corrected
  - Table 9 changed
  - Chapter 4.4 changed
  - Chapter 4.5 changed
- V 0.0.14: Consolidation after meeting #12
  - Chapters 4.1.2 and 4.1.3 changed
  - Figure 2 changed
  - Reference format aligned
  - References updated
  - Spelling corrections
- V 0.0.15: Editing in meeting #14, consolidation after meeting #14
  - Table 9 changed
  - Chapter 3.3.1 changed
  - Chapter 4.3.2.1: New chapter headline
  - Chapter 4.3.2.2 added
  - Chapter 4.4.2 added
  - Chapter 4.4.3 changed: Headline and content
  - Annex A added
- V 0.0.16: Editing before and in meeting #15, consolidation after meeting #15
  - Action items #14-2 and #14-3: review of terms and abbreviations
  - Chapters 4.1.3 and 4.3 revised
  - Introduction of Security Profile D
  - Various editorial changes
- V 0.0.17: Editing before, in and after meeting #16
  - Table changed
  - Chapters 4.3.3 and 4.3.4 changed
  - Annex A: Nonce in examples corrected
  - Editorial changes: abbreviations aligned
- V 0.0.18: Editing before, during and after meeting #18
- V 1.0.0: Editing before, during and after meeting #19, release candidate
- V 1.0.1: Consideration of OMS review comments, release

Contents

Tables

Figures

Preface

This document specifies OMS over mioty, which is a method to use mioty as a transport mechanism in an OMS network. It was created in a joint task force with members of OMS and the mioty alliance.

This document is aimed at readers who want to implement or understand OMS over mioty specifically. It is assumed that the reader is reasonably familiar with the mioty and OMS technologies by themselves, and has access to working implementations of both. The document gives only introductory descriptions of the concepts and interfaces where the two technologies interact, e.g. device addresses, the MAC layer of mioty, or the M-Bus Adaptation Layer (MBAL). It then specifies those interactions in detail. For further details on the individual technologies, please refer to their respective specifications, as they are not in scope of this document.

1 Introduction

The [EN 13757] “Communication Systems for Meters” standard series specify several communication layers including both the “upper layers” of OSI model (transport, authentication and fragmentation, and application layers) and “lower layers" (physical, data link, extended link and medium access layers). Upper layers can be transported both over wired and wireless links as specified in the “lower layers”.

Mioty is an LPWAN (Low Power Wide-Area Network) wireless communication protocol based on TS-UNB (Telegram Splitting Ultra Narrowband) as described in [ETSI 103 357], intended for massive IoT deployments and is suitable for battery powered devices. It is a point-to-point protocol to exchange data directly with a communication partner (gateway).

This document proposes an architecture for a combined protocol to transport [EN 13757] higher layers over the mioty lower layers. The layered structure of the combined protocol, referring to the OSI model, is depicted in the following Table 2 in chapter 4.1.

2 Glossary of Terms

Additional terms and clarifications to [OMS-S1], Annex A.

Table 1 – Glossary table

Term	Description
A	**A**
AC, Application Center	Entity receiving and / or transmitting data from and / to the OMS end-devices through a mioty network.
ACC-DMD	Access Demand
ACK	Acknowledgement
AES	Advanced Encryption Standard
AES-CTR	Advanced Encryption Standard - Counter Mode
A-Field	Address Field
AFL	Authentication and Fragmentation Layer
AFLL	AFL-Length Field
AMM	Automated Meter Management
AMMHES	AMM Head-End System
APL	Application Layer
APP	Application
B	**B**
B-Field	Bi-directional subfield in Extended Link Layer Communication Control field
BS, Base Station	Device receiving radio signals from the end device and interfacing to a Service Center
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSSCI	Base Station Service Center Interface
C	**C**
CBC	Cipher Block Chaining
CC-Field	Communication Control Field
CF	Configuration Field
CFE	Configuration Field Extension
C-Field	Control Field containing the FCB and FCV bits and other control information
CI-Field	Control Information Field, contains the type of command sent (set baud rate, application reset, select slave, etc.)
CMAC	Cipher-based Message Authentication Code
CMD	Command
CNF-IR	Confirm Installation Request
D	**D**
D-Field	Response Delay subfield in Extended Link Layer Communication Control field
DIB	The Data Information Block contains one DIF and zero to ten DIFEs for the length, type and coding of the data – also see VIB
DIF	Data Information Field – control field – element of the M-Bus datapoint, for the resolution and additional control elements
DIFE	Data Information Field Extension, contains additional information such as tariff or subunit of the device; see: DIF
DLL	Data Link Layer

Term	Description
Downlink	mioty telegram sent from the Network Server to the OMS end-device
DT	Device Type
DV	Device Version
E	**E**
ED	End Device: A meter/actuator, radio adapter or sensor, according to mioty definition, that implements this TR recommendations.
ELL	Extended Link Layer
ELL-CC	Extended Link Layer-Communication Control Field
F	**F**
FCB	Frame Count Bit is a toggling bit, signalling if data blocks are repeated due to an error condition (bit not changed) or in correct order.
FCL	Fragmentation Control Field
FCV	Frame Count Valid bit signals whether the frame count mechanism is active
G	**G**
H	**H**
I	**I**
ID	Identification Number
IoT	Internet of Things
J	**J**
K	**K**
L	**L**
LLC	Logical Link Control
LPWAN	Low Power Wide-Area Network
LSB	Least Significant Byte
LTN	Low Throughput Networks
M	**M**
MAC	Media Access Control
MBAL	M-Bus Adaptation Layer
MBAL-CL	MBAL control field
M-Bus	Meter-Bus
MCL	Message Control Field
MCR	Message Counter Field
MF	Manufacturer field
MPDUCNT	MAC Payload Data Unit Counter
MPF	MAC Payload Format Field
MSB	Most Significant Byte
MSK	Minimum-shift keying

Term	Description
N	**N**
NACK	Negative Acknowledgement
NWK	Network
NWKKey	Network-Key
NWKSKey	Network Session Key: AES 128 Key material used to authenticate, encrypt and check the integrity of LoRaWAN packets
NWL	Network Layer
O	**O**
OMS	Open Metering System
OSI model	Open Systems Interconnection model
OTAA	Over the air attachment
P	**P**
PHY	Physical Layer
Q	**Q**
R	**R**
REQ-UD1	Requests User Data (class 1)
REQ-UD2	Requests User Data (class 2)
RFU	Reserved for Future Use
RSP-UD	Response with user data
S	**S**
SC Service Center	Entity managing Base Station in a LTN Network and forwarding data traffic from the network to the Application Center and back
SCACI	Service Center Application Center interface
SIGN	Signature
SITP	Security Information Transfer Protocol
SND-IR	Send Installation Request
SND-NR	Send No Reply
SND-UD	Send User Data
STS	Status
T	**T**
TLS	Transport Layer Security
TPL	Transport Layer
TR	Technical Report
TS	Telegram Splitting
TSMA	Telegram Splitting Multiple Access
TS-UNB	Telegram Splitting Ultra Narrowband
U	**U**
UNB	Ultra-Narrowband
Uplink	A mioty packet sent from the OMS end-device to the mioty BS
User	A person who designs, installs or starts up M-Bus installations in the field.
V	**V**

Term	Description
VIB	The Value Information Block contains one VIF and zero to ten VIFEs
VIF	Value Information Field. Element of the M-Bus protocol used to define units and scaling factor of a datapoint and additional information.
VIFE	Value Information Field Extensions. Adds information to the VIF (e.g. m3), such as “per hour” or an error status or actions to be performed (e.g. clear data).
W	**W**
X	**X**
X-Field	Extended Delay subfield in Extended Link Layer Communication Control field
Y	**Y**
Z	**Z**

3 References

For dated references only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[ETSI 103 357] Short Range Devices; Low Throughput Networks (LTN); Protocols for radio interface A, v 1.1.1:2018-06

[ETSI 103 358] Short Range Devices; Low Throughput Networks (LTN) Architecture; LTN Architecture, v 1.1.1:2018-06

[EN13757-3] EN 13757-3:2018 Communication systems for meters – Part 3: Application protocols

[EN13757-4] EN 13757-4:2019 Communication systems for meters – Part 4: Wireless M-Bus communication

[EN13757-7] EN 13757-7:2018 Communication systems for meters – Part 7: Transport and security services

[prEN13757-8] EN 13757-7:2018 Communication systems for meters – Part 8: Adaptation Layer; January 2021

[M-AS] mioty Application Layer Specification, v 1.0.0

[OMS-S1] OMS Specification Volume 1, General Part, Issue 2.3.1 including Annex A, Release E, https://oms-group.org/open-metering-system/oms-spezifikation

[OMS-S2] OMS Specification Volume 2, Primary Communication, Issue 4.5, https://oms-group.org/open-metering-system/oms-spezifikation

4 General Layer structure

4.1 Overview

This document proposes an architecture to transport EN 13757 “upper layers” over the mioty “lower layers”. In-between is the M-Bus adaptation layer that is defined to transport M-Bus datagrams over LPWAN technologies. The general layer structure of this mechanism is depicted in Table 2.

Table 2 - OMS over mioty general layers structure

OSI Model	M-Bus Layer Model	mioty Layer Model	Layers for OMS over mioty	
Application Presentation	**APL (EN 13757-3)**	mioty APL [c]	**APL**	**M-Bus Upper layers**
Session Transport	**TPL (EN 13757-7)**		**TPL**	
	AFL (EN 13757-7)		**AFL**	
Adaptation [a]	**MBAL (EN 13757-8)**		**MBAL**	
Network	NWL (EN 13757-5)			**mioty Lower layers**
Data Link	ELL (EN 13757-4)	**TS-UNB-LLC** [b]	**TS-UNB-LLC**	
	DLL (EN 13757-2/-4)	**TS-UNB MAC** [b]	**TS-UNB MAC**	
Physical	PHY (EN 13757-2/-4)	**TS-UNB PHY** [b]	**TS-UNB PHY**	

[a] Adaptation layer is an extension of the original OSI model for the purposes of M-Bus over LPWAN
[b] As specified in [ETSI 103 357]
[c] As specified in [M-AS]

4.2 M-Bus Application over Mioty

A valid mioty frame always consists of the PHY and MAC layer. On top there are either

- just LLC information or
- just MBAL and upper layer information (without LLC) or
- LLC, MBAL and upper layer information.

The MBAL and upper layers, if present, are introduced by the MPF field of the TS-UNB MAC (see 4.3). The MBAL is only one byte as explained in [prEN 13757-8]. It is followed by specific CI-Field values as explained in [EN 13757-7]. The usage of the upper layers shall comply with [EN 13757] standard and OMS specifications rules.

The MBAL provides missing services of the M-Bus lower layers when M-Bus upper layers are transported over an LPWAN technology. It is defined precisely for purposes like OMS over mioty. The missing services are:

- the message type (the function code of the C-Field)
- the accessibility (the A- and B-Field of the ELL-CC)
- the latency (new function, replacing the D- and X-Field of the ELL-CC)

All these services are coded in the one-byte MBAL-CL field (the MBAL control field). The subfields are explained in 6.2.

Typically only the payload of a LPWAN technology is forwarded to the application. With the MBAL (as first byte of the payload) the missing service information reaches the application. An example is a REQ-UD2 that just contains TPL data as upper layer payload. Without the function code information of the MBAL, the OMS end-device (application module) does not know about the intention of this message.

The latency provides the possibility to inform the end point application about the expected reaction time.

4.3 MAC Payload Format Field

The MAC payload format field (MPF) of the TS-UNB MAC (see mioty frame structure in 5.3) indicates the format of the MAC payload. It is optional in the mioty layer model but mandatory for OMS over mioty.

OMS over mioty shall use MPF value 83_h. That value indicates that the first byte of the MAC payload is the MBAL-CL field of the Short MBAL according to [prEN 13757-8]. The optional MBAL CI-Field shall be omitted.

MPF value 80_h shall not be used for OMS over mioty. That value indicates that the first payload byte is an M-Bus CI-Field that describes the further payload content. It allows a very flexible transport of any sort of M-Bus data over mioty. In OMS over mioty however, all packets shall contain the MBAL. Therefore using MPF value 83_h saves one byte compared to MPF value 80_h (the additional MBAL CI-Field with value CF_h).

5 Overview mioty architecture

5.1 General explanation of mioty

Mioty is a Low Power Wide Area Network (LPWAN) technology based on the Telegram Splitting Ultra Narrowband (TS-UNB) protocol family defined in ETSI specification [ETSI 103 357]. This specification covers PHY, MAC and LINK Layer of the TS-UNB protocol. Additional radio protocol settings and application layer specification for interoperability is defined in the mioty alliance.

Mioty and TS-UNB transmission technology are using a novel channel access method called Telegram Splitting Multiple Access (TSMA) which is used for transmission from the end-device to the Base Station (Uplink) and back (Downlink) – mioty is therefore bidirectional. In the TSMA method, the data packets are divided into several small sub packages (radio bursts) and transmissions of radio packets are distributed in frequency and time over the radio channel.

Mioty supports unidirectional (Class Z) from the end-device to the Base Station and bidirectional communication (Class A). Class A communication is always initiated by the end-device, hence any Downlink can only be executed after a fix delay time after an Uplink. Although there are two specified modulation rates in the TS-UNB protocol, mioty only supports the Ultra Low Power -mode (ULP mode) with a symbol rate of 2380,371 Sym/s. Hence it realizes a high coupling loss of 153 dB at a short on-air time of 1,95 ms per Bit (PHY Payload).

Each mioty end-device is identified by a unique IEEE EUI64 identifier and the MAC Payload is encrypted with AES128 and an individual 128 Bit Network key.

5.2 Architecture

The network architecture of mioty is based on the Low Throughput Networks (LTN) architecture described in [ETSI 103 358]. The architecture includes a Service Center (SC), at least one Base Station (BS) and a number of end-devices (ED). The end-devices communicate with the Base Stations by Radio Frequency link. A packet from the end device (Uplink) can be received by one or more Base Stations, while a packet to the end device can only be transmitted from one Base Station at a given time. The end-devices and Base Stations are managed by a central unit called the Service Center. An end-device sends its application data message end-to-end encrypted via the Base Stations and the Service Center to a remote counterpart called Application Center (AC) and vice versa. The data exchange in mioty networks is shown in Figure 1.

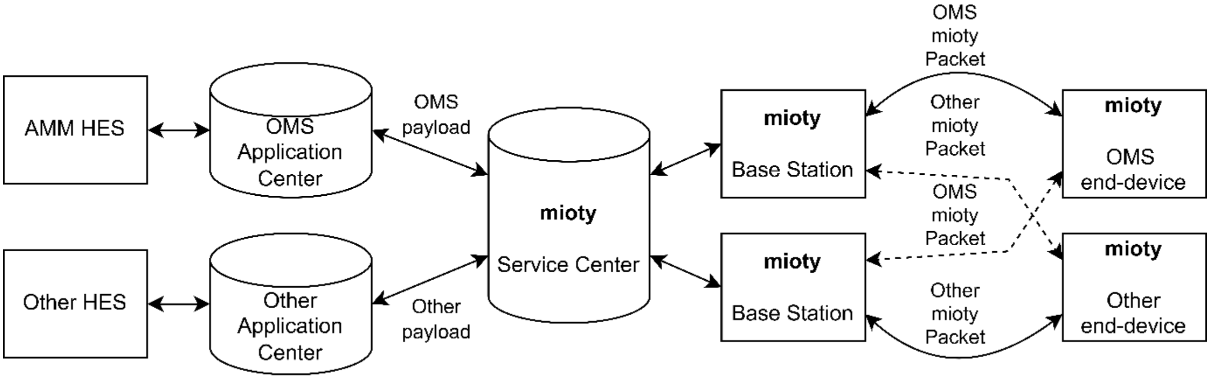

Figure 1 - Network Architecture of mioty (data exchange)

The interface between a Base Station and a Service Center is called BSSCI and is specified in the mioty alliance. The interface between Service Center and Application Center is called SCACI. Service Center and Application Center can be merged as one entity.

5.3 Introduction of frame structure

The TS-UNB specification has two protocol options:

- Fixed MAC covering PHY, MAC and LINK layer
- Variable MAC covering PHY-layer only and allows the use of other MAC and LINK layers

OMS over mioty uses fixed MAC only.

5.3.1 Uplink Frame

The Uplink transmission frame consists of a core frame that can contain up to 10 bytes of application data. A minimum of 24 radio bursts are transmitted in the core frame. For larger application data of up to 245 bytes, an optional extension frame is appended that contains the additional data. For each additional byte of application data to be transferred, an additional radio burst is attached to the extension frame. The distribution of radio bursts in time and frequency is defined by TSMA-pattern.

Table 3 – mioty Uplink MAC Format

Field	MAC Header	Address	MPDUCNT	MPF	MAC Payload	SIGN
Size (Bytes)	1	2/8	3	0/1	1-245	4

The MAC Format consists of the following fields:

- **MAC Header:** The MAC Header contains Flags for controlling the MAC
- **Address:** Contains the end-device address as 16 Bit Short address or the full unique EUI64 address
- **MPDUCNT:** contains the 24 Bit counter value of a 32 Bit message counter stored in the end-device and in the Base Station
- **MPF:** optional field to identify the format of the MAC Payload data
- **MAC Payload:** contains Control and/or Data payload
- **SIGN:** CMAC for message authentication

Table 4 – Uplink MAC Header Field

MS Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
MAC-Version	MPF Flag	Control Flag	Response Flag	RX Open Flag	Addressing mode	Attach Flag	ACK
Version of the MAC (0=Initial Version)	Set to 1 if MPF field is used	Set to 1 if MAC Payload contains Link Layer Control field	Set to 1 if end-device expects Downlink message	Set to 1 if end-device opens a receive window for Downlink reception after Uplink	Set to 0 if 16 Bit short address is used	Set to 0 for regular transmission, and set to 1 for attachment together with other settings	Set to 1 for acknowledge of previous Downlink reception

5.3.2 Downlink Frame

In downlink a transmission frame consists of a core frame and an optional extension frame. The Base Station is transmitting the data in blocks of 18 radio bursts. The size and transmission duration of a radio burst varies depending on the MAC payload data. The Downlink telegram can handle 1 to 250 bytes of application data.

Table 5 – mioty Downlink MAC Format

Field	MAC Header	MPF	MAC Payload	SIGN
Size (Bytes)	1	0/1	1-250	4

The MAC Format consists of the following fields:

- **MAC Header**: The MAC Header contains Flags for controlling the MAC
- **MPF:** optional field to identify the format of the MAC Payload
- **MAC Payload:** contains Control and Data payload
- **SIGN:** CMAC for message authentication

Table 6 – Downlink MAC Header Field

Bit	Field	Description
MS Bit 7	MAC-Version	Version of the MAC (0=Initial Version)
Bit 6	MPF Flag	Set to 1 if MPF field is used
Bit 5	Control Flag	Set to 1 if MAC Payload contains Link Layer Control field
Bit 4	Response Flag	Set to 1 if Base Station expects Uplink message
Bit 3	RX Open Flag	Set to 1 if Base Station want to send further Downlink messages and requests end-device to open a further receive window after next Uplink
Bit 2	Response Priority Flag	Set to 1 if end-device response is expected within a priority time window of 120 s
Bit 1	RFU	Reserved for future use (shall be set to 0)
LS Bit 0	RFU	Reserved for future use (shall be set to 0)

6 Technical Realisation

6.1 Address handling

6.1.1 M-Bus Address

M-Bus use a unique 8 Byte address to identify end-devices (meters, actuators, sensors, adaptors and concentrators). This address contains the following 4 fields:

- a two-byte Manufacturer ID that ensure the uniqueness of addresses that are managed by each manufacturer. This field is managed by the flag association, UK see [EN 13757-7:2018], 7.5.2.
- a four-byte BCD coded ID as specified in [EN 13757-7:2018], 7.5.1.
- a one-byte version field as specified in [EN 13757-7:2018], 7.5.3.
- a one-byte device type as specified in [EN 13757-7:2018], 7.5.4.

In M-Bus this address is used in the link layer (DLL) as a "from" address, in the extended link layer (ELL) as a "to" address, or in the transport layer (TPL) as an application address (end point identifier).

6.1.2 Mioty Address

Mioty uses a unique 8 Byte address to identify devices (mioty device address, in mioty called end-point), which is an EUI64 address (Extended Unique Identifier) managed by IEEE. IEEE offers different address ranges with different sizes of the OUI (Organisationally Unique Identifier) ensuring the uniqueness of addresses between manufacturers.

Further, in mioty the unique device address used by the link layer in Uplink direction may be replaced by a 16-bit short address (mioty short address) when transmitted over-the-air to achieve a more compact frame. This short address is always related to a mioty device address and either pre-assigned or assigned by the Service Center during the attachment of the end-device to the mioty network. In Downlink direction the short address is entirely omitted as the reception window itself will indicate the end-device being addressed, and verified by the signature check. This is to keep the Downlink frames as compact as possible.

6.1.3 Relation between M-Bus Address and mioty Address

Even if both M-Bus and mioty device addresses are 8 Bytes long, they cannot be interchanged as that would compromise the uniqueness. Therefore, the mioty device address and the M-Bus address are inherently independent.

When M-Bus upper layers are transported over mioty lower layers, the link and MAC layers use the unique mioty device address or the mioty short address. The upper layers use the M-Bus address contained in the TPL. The relationship between the mioty device address and the M-Bus application address can be announced by transmitting the application address at least during the installation procedure (see 6.3.5) inside the long TPL according [EN 13757-7:2018], 7.4.

If there is a 1:1 relation between the unique mioty device address and the application address that has been announced successfully to the Application Center, then the transmission of the application address may be skipped in any later message transfers. Otherwise, the application address needs to be provided at any time.

It is the responsibility of the Application Center to keep the mapping(s) of the mioty and M-Bus address after the installation procedure (see 6.3.5.1).

6.2 Usage of M-Bus Adaptation Layer (MBAL)

6.2.1 Subfield Version

The Version subfield shall be set to 00_b to indicate version 1 of the MBAL.

6.2.2 Subfield Access (Uplink)

The Access subfield in the MBAL replicates the A-Field and B-Field of the CC-Field in the Extended Link Layer (see [EN 13757-4], 13.2.7.2 and 13.2.7.7). It shall be used according [prEN 13757-8], Table 30: "End-Point Access mapped to Device Class".

Class Z devices shall use access value 00_b to indicate No Access.

Class A devices shall use access value 01_b during their installation procedure (see 6.3.5.1). Class A devices that are in the end-device status "Installed" (see 6.3.2) may use access value 01_b to indicate limited access. Class A devices in a different end-device status shall use access value 00_b to indicate No Access.

In case of security mode 0 or 5 there are several link control bits located in the TPL Configuration Field (see [OMS-S2], 5.3.3). All these bits (B, A, S, R, H) shall be ignored if the MBAL is present.

If Value 00_b is used, the RX Open Flag may be cleared in the mioty header of the uplink. If Value 01_b is used, the RX Open Flag in the Uplink shall be set and the end-device shall open a downlink reception window after uplink

6.2.3 Subfield Latency (Downlink)

The latency subfield in the MBAL offers functionality similar to the D-Field and X-Field of the CC-Field in the Extended Link Layer. It defines the expected latency for the OMS end-device response. It is independent from the Response Priority Flag of the Downlink MAC Header Field as it is directed to the upper layers. The following table details which MBAL latency can be used for OMS over mioty and what is the expected behaviour.

Table 7 – Latency for OMS over mioty

MBAL Subfield Latency	MBAL Description	Usage for OMS over mioty
00_b	RFU	Shall not be used
01_b	Response or TPL ACK can be sent with delay.	The end-device shall answer within 1 hour.
10_b	Response or TPL ACK is expected as soon as possible.	The end-device shall answer within 2 minutes. [a]
11_b	Unused or invalid	The system does not require a certain latency or an answer from the end-device upper layers is not expected.
[a] Just in case lower layer restrictions (e.g. a duty cycle limitation) do not permit answering within 2 minutes the end-device shall provide the answer as soon as possible.		

6.2.4 Subfield Function Code

The Function Code subfield in the MBAL replicates the function code in the C-Field of the Data Link Layer. The following tables detail which MBAL function code shall be used to replicate the equivalent C-Field value.

Table 8 – Mapping of C-Field to MBAL Function Code for Uplink

C-Field specified in [OMS-S2]		Equivalent Function code to be used in MBAL	
SND-NR	44h	SND-NR	4h
SND-IR	46h	SND-IR	6h
ACC-DMD	48h	ACC-DMD	Ah
ACK	00h, 10h, 20h, 30h	TPL-ACK	0h
NACK	01h, 11h, 21h, 31h	TPL-NACK	1h
RSP-UD	08h, 18h, 28h, 38h	RSP-UD	8h

Table 9 – Mapping of C-Field to MBAL Function Code for Downlink (BS)

C-Field specified in [OMS-S2]		Equivalent Function code to be used in MBAL	
SND-UD2	43h	SND-UD2	3h
SND-UD	53h, 73h	SND-UD	2h
REQ-UD1	5Ah, 7Ah	REQ-UD1	Ah
REQ-UD2	5Bh, 7Bh	REQ-UD2	Bh
ACK	00h	TPL-ACK	0h
CNF-IR	06h	CNF-IR	6h

The usage of the C-Field is specified in [OMS-S2], 5.2.

Function codes that are defined in [EN 13757-8] or elsewhere but are not listed in Table 8 and Table 9 shall not be used in OMS over mioty.

The function code TPL-NACK in the Uplink is used by the end-device to indicate that it does not support the received function code. [OMS-S2] also lists a meter reception buffer overflow as a possible use case, but OMS over mioty end devices should avoid this by providing sufficiently large reception buffers (i.e. 255 bytes).

6.3 Installation / Deinstallation

6.3.1 General

An OMS over mioty end device needs to be provisioned in a mioty network, attached to that same network, and installed in the AMMHES. Figure 2 provides an overview of this procedure for a Class A OMS end-device. The following paragraphs describe the process steps and the resulting device statuses.

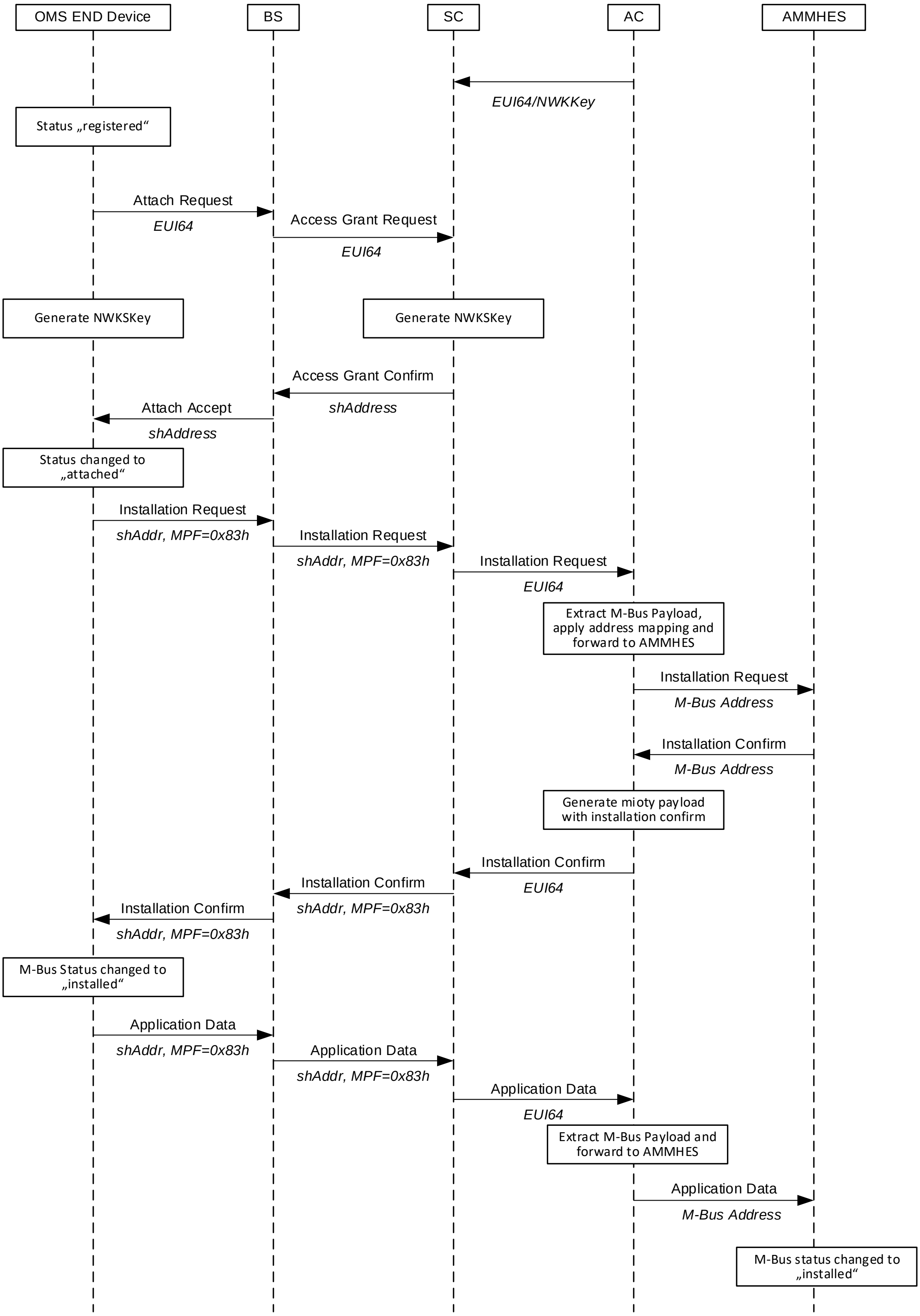

Figure 2 – Attachment and Installation procedures for a Class A OMS over mioty end device

6.3.2 Device Status

The mioty end device can have statuses according to the following Table 10.

Table 10 – End Device Status

End Device Status	Description
Registered	A device that is provisioned to a certain mioty network. Class A devices may start in this status if they use over the air attachment.
(Pre-)Attached	A device that has a valid short address and network session key. It is now ready to send and/or receive data through a specific mioty network. Attachment may happen through an over the air attachment procedure for Class A devices, or through Pre-Attachment (optional for Class A devices, mandatory for Class Z devices). Pre-Attached devices start in this status. Attached or Pre-Attached devices can transmit messages to the AMMHES, using the long TPL header format. They cannot receive messages from the AMMHES.
Installed	An attached mioty end device changes to the installed status after sending an installation request and receiving an installation confirm from the AMMHES. The installation request is usually sent after the end device has been physically installed at its final position. Installed devices can transmit and receive messages to and from the AMMHES, using the short or long TPL header formats.
Detached -> Registered	End devices that use the over the air attachment procedure can detach from the mioty network. The network session key, the application session key and the short address are then no longer valid and the device goes back to the registered status.

6.3.3 Mioty Provisioning

A mioty end device has an unique EUI64 identifier and a network key. To register a device in a mioty network, that EUI64 and network key are provided to the Service Center of the mioty network. A Base Station connected to the Service Center gets access to this information whenever it is needed for the communication with this end device. After a successful provisioning the end device has the status “registered”.

6.3.4 Mioty Attachment

In order to transmit and receive data in a mioty network, the end device needs to be attached to the network. During attachment, the end devices short address and network session keys are shared between the end device and the mioty Service Center. This can happen either offline as a Pre-Attachment, or online through an “over the air attachment” (OTAA) procedure.

Pre-attached devices have a fixed short address that is programmed into the device, and use their network key as their network session key. Pre-attachment is done by uploading the short address, the EUI64 and the network key to the Service Center during a combined mioty provisioning and pre-attachment process. Pre-attached devices are immediately ready to transmit data over the network. Class Z devices shall be pre-attached, because they are unidirectional and do not support the OTAA procedure.

Class A devices may be pre-attached, or may attach itself to the network by running an “over the air attachment” procedure. A network session key is derived from the network key and a short address is generated. Both will be stored in the end device and the Service Center, and distributed to the connected Base Stations. After the successful mioty attachment procedure the OMS end-device has the status “attached”.

6.3.5 Installation Procedure

6.3.5.1 Installation Procedure for Class A devices

After the mioty provisioning and attachment of a bidirectional OMS end-device to a mioty network, it may start the OMS installation procedure to announce a mapping between the mioty EUI64 and M-Bus address (see Figure 2).

In case of an 1:1 relation between mioty EUI64 and M-Bus address, it may do it once (e.g. a plug in RF-adapter). In case of an 1:n relation between mioty EUI64 and M-Bus addresses, it may do it individually for each M-Bus address (e.g. a wired M-Bus to mioty adapter connecting several wired M-Bus devices).

To announce a mapping, the end device shall transmit a SND-IR packet. It shall use the long TPL header that contains the full M-Bus address of the meter according to [EN13757-7:2018], clause 7.4.

On the MAC layer, if a packet is transmitted with the mioty short address the mioty Service Center maps that short address to the device’s full EUI64. The Service Center passes the full EUI64 address together with the payload to the Application Center.

The Application Center shall store the mapping between that EUI64 and the M-Bus address for future reference. If it already has mappings with the same EUI64, but different M-Bus addresses, those mappings shall be kept. All mappings shall be marked in a way to ascertain the order in which mappings with the same EUI64 were received (e.g. a timestamp of their reception or a running index). If the Application Center already has a mapping for the same M-Bus address, but a different EUI64, that pre-existing mapping shall be discarded.

The OMS Installation Request (SND-IR) with the M-Bus Address is then passed on to the AMMHES. The AMMHES shall respond with a CNF-IR message addressed to the OMS end-device. The Application Center uses the stored mapping to find the corresponding mioty EUI64 address and generates an OMS over mioty packet addressed to that EUI64. It is then passed on to the Service Center for transmission.

Once the end device receives the CNF-IR message, it changes to status “Installed”. Please note that not all OMS end-devices are required to run the installation procedure and will therefore not reach the status “Installed”. OMS end-devices in the status “Installed” may use the short TPL header that does not contain the full M-Bus address in subsequent OMS over mioty packets.

When the Application Center receives an OMS over mioty packet that does not contain an M-Bus address in the TPL header, it shall check if an address mapping has been stored for that EUI64. If one mapping is found, the Application Center shall pass the message on to the AMMHES with the M-Bus address. If several mappings are found, only the most recently received mapping shall be used. If no such mapping is found, the Application Center shall discard the message.

OMS over mioty end-devices with several address mappings shall always use the long TPL header as to avoid misattributions of packets to the wrong M-Bus sender address.

Messages from the AMMHES can only be forwarded if there is an address mapping in the Application Center. The AMMHES passes the message to the Application Center. The Application Center shall then check if it has exactly one mapping for that M-Bus address. It shall then forward the packet to the referenced EUI64. If no such mapping is found, the Application Center shall discard the message.

6.3.5.2 Installation procedure for Class Z devices

6.3.5.2.1 General

In the installation procedure described above, the AMMHES transmits an installation confirmation to the end device. For Class Z devices, which support only uplink communication, this is not feasible.

This document does not specify an installation procedure for Class Z devices. It does however list some solutions that implementers may choose to use:

6.3.5.2.2 Using a side channel to install the device

Class Z devices are pre-attached to the mioty network by uploading their EUI64 and network key to the Service Center directly in the provisioning process. Implementers may choose to install the mapping between the EUI64 and M-Bus address offline as well. In some use cases, where the mapping between the EUI64 and M-Bus address does not change during the life time of the device, this approach is feasible. In others, e.g. for pluggable RF adapters, it may not be.

6.3.5.2.3 Transmitting the M-Bus address in every packet

The installation procedure establishes a mapping between the EUI64 and M-Bus address so that the M-Bus address may be omitted in subsequent packets (see 6.1.3). That mapping is not needed if the M-Bus address is transmitted in every uplink packet. This uses more payload data, and in turn may reduce the life time of battery powered devices.

6.3.5.2.4 Conducting the online Installation Procedure with no confirmation

In the Installation Procedure described above, the end device sends an Installation Request, waits for a confirmation, and changes into the “registered” state once it has been received. Implementers may choose to adapt this procedure to Class Z devices. The end device would transmit the Installation Request (possibly with repetitions in pre-defined time intervals) and then change into the “installed” state without expecting a confirmation. This approach requires that there are ways to verify if the online Installation has succeeded and to intervene if it fails. The feasibility of this approach is very dependent on the use case.

6.4 Data Exchange

6.4.1 Type of Messages

As the OMS end-devices will be connected to mioty networks, the M-Bus link layer will not be used. To keep the M-Bus data exchange principles effective the MBAL as described in chapter 4.2 shall be applied. The Function Code inside the MBAL Control Field is used to describe the type and function of a message. Its meaning corresponds to the Function Codes of the C-Field which is part of the M-Bus link layer.

The mioty protocol offers the possibility to influence the response behaviour of the communication partner in both directions with the “Response flag” bit inside the MAC header. As the response behaviour is independent from the use case “OMS over mioty” this bit is set to 0 per default.

6.4.2 MAC Services

As explained in 5.3 only fixed MAC is applicable for OMS over mioty. The MAC format and MAC header for Uplink and Downlink is described in section 5.3.1 and 5.3.2 respectively. OMS end-devices use the mioty MAC functions and procedures exactly as described in [ETSI 103 357].

6.4.3 Link Layer Services

To establish and maintain a connection between an OMS end-device and a Base Station a set of Link Layer Control Commands are available. The control flag in the MAC Header shall determine whether a control payload is present in the MAC or not. The control payload comprises one or more control segments according to [ETSI 103 357], 6.2.2.2. The Link Layer Control Commands can be transmitted either along with an application message or separately, which means without application data.

OMS end-devices use the mioty link layer services exactly as described in [ETSI 103 357]. An example is the attach service as shown in 6.3.5.

6.4.4 Devices Classes

As explained in 3.1 there are two device classes for mioty. Both are applicable for OMS over mioty.

In case the two different classes need specific treatment it is explained in the respective chapters individually.

6.4.5 Message Content of an OMS end-device

The OMS end-device shall provide M-Bus data points according to [OMS-S2], 8.4.4.

6.5 Security Options

6.5.1 Security Mechanisms Overview

Every OMS end-device using a mioty network shall comply with the mioty security mechanisms specified in [ETSI 103 357]. This is a network related security mechanism between the mioty end-device and the mioty Base Station where each mioty packet is encrypted, origin authenticated, and integrity protected.

For OMS end-devices an end-to-end security (up to the application center) shall be added by applying supplementary security mechanisms provided by the respective OMS security profile (see 6.5.3).

Additional application layer security as defined by the mioty alliance shall not be used.

6.5.2 mioty Security

The mioty radio protocol requires mandatory network related security mechanism to ensure the following security properties:

- Integrity and origin authentication:
  Every mioty Uplink packet exchanged on the network carry a signature field (SIGN) for integrity check. These 4 bytes AES-CMAC-Field calculated using the NWKSKey, guarantee that the mioty packet has not been tampered during transmission and enables the receiver to prove the authenticity of the packet. The SIGN field is described in [ETSI 103 357], 6.3.2.3.5. In Downlink a 6 byte AES-CMAC signature calculated using the NWKSKey is used as synchronisation word on PHY layer. The NWKSKey is derived from the preprovisioned NWKKey after an over-the-air attachment procedure. In the case of an unidirectional end-device, the NWKKey is always used as a NWKSKey
- Network confidentiality:
  The MAC Payload of every mioty packet is encrypted using an AES-CTR algorithm together with the NWKSKey (see [ETSI 103 357], 6.3.2.6.1). It ensures over-the-air confidentiality between the gateway and the OMS end-device.
- Replay protection:
  A 24 Bit Message Counter (MPDUCNT) is contained in each mioty Uplink packet (see [ETSI 103 357], 6.3.2.2.4). It is incremented for each new MAC payload. The Message Counter is part of the CMAC calculation. It enables the receiver, which keeps track of the value, to detect replayed packets. In Downlink no message counter is explicitly included in the transmitted packet, but the message counter of the corresponding Uplink message is part of the Downlink CMAC calculation.

6.5.3 Security by M-Bus

Any OMS over mioty end device shall provide end-to-end security by using one of the M-Bus TPL security services of Table 11 according to its application needs in addition to the mioty network security. The OMS security profiles are defined in [OMS-S2], Table 40.

Table 11 - TPL security for OMS end-devices

OMS Security profile	Description	Applicable for OMS over mioty end device
No Security profile	This profile has no security services.	NO, as end-to-end security is not ensured
Security Profile A	Provides end-to-end confidentiality by a symmetric encryption	YES [a]
Security Profile B	Providing end-to-end confidentiality, authenticity and integrity by symmetric technologies	YES [a]
Security Profile C	Providing end-to-end confidentiality, authenticity and integrity by a TLS session over mioty	YES [a]
Security Profile D	Providing end-to-end confidentiality, authenticity and integrity by symmetric AES-CCM technology	YES [a]
[a] Messages without application data can apply security mode 0.		

An OMS over mioty end device may use additional APL security (up to the AMMHES) according to [OMS-S2], 9.4.2, Table 44.

Key exchange of the master key in case of symmetric Security profiles A, B or D shall be handled according to [OMS-S2], Annex M.

Key exchange in case of Security profile C shall be handled according to [OMS-S2], Annex F.

6.5.4 Security versus Packet Length

The size of an OMS over mioty packet depends on the number of payload bytes and on the selected security profile of the upper layer. The size of the MAC payload increases as can be seen in Table 12.

Table 12 - Security overhead (in Bytes) by security profiles

	Layer dependent overhead						Payload size (MAC Payload)		
Security profile	MBAL	AFL	TPL	SITP	TLS	Padding Bytes	MAC Payload	MAC Payload	MAC Payload
M-Bus APL							10	40	120
SP_A (short TPL)	1		7			4 / 6 / 6	22	54	134
SP_A (long TPL)	1		15			4 / 6 / 6	30	62	142
SP_A (long TPL) + ASP10	1		15	26		10 / 12 / 12	62	94	174
SP_B (short TPL)	1	17	8			4 / 6 / 6	40	72	152
SP_B (long TPL)	1	17	16			4 / 6 / 6	48	80	160
SP_B (long TPL) + ASP10	1	17	16	26		10 / 12 / 12	80	112	192
SP_C (short TPL)	1		6		53	6 / 8 / 8	76	108	188
SP_C (long TPL)	1		14		53	6 / 8 / 8	84	116	196
SP_C (long TPL) + ASP10	1		13	26	53	12 / 14 / 14	115	147	227
SP_D (short TPL)	1		19				30	60	140
SP_D (long TPL)	1		27				38	68	148
SP_D (long TPL) + ASP10	1		27	26			64	94	174

Table 12 gives the resulting MAC Payload size (Bytes) for three APL sizes (10, 40 and 120 Bytes) for different Security Profiles, different TPL headers (short or long) and optional application security (here ASP10). It shows that the overhead has to be taken into account, especially if application security is applied on top. Nevertheless, all of these sizes can be transported in uplink or downlink direction without the need for AFL fragmentation, which means, it can be transported in one packet (see MAC payload sizes of Table 3 and Table 5).

Annex A (informative): OMS over mioty Frame Examples

A.1 Overview Table

Table A.1 – List of examples

Example Name	Chapter	OMS Security Profile
Gas meter example		
General parameters	A.2	
SND-IR	A.3	A
CNF-IR	A.4	A [a]
Gas meter example		
General parameters	A.5	
SND-NR	A.6	B
Water meter example		
General parameters	A.7	
SND-UD Correction of time	A.8	A
ACK	A.9	A [a]
SND-UD2 Correction of time	A.10	A
RSP-UD Empty response	A.11	A [a]
[a] Messages without application data can apply security mode 0.		

A.2 General Parameters

Table A.2 – General parameters

Gas meter example	
Medium	Gas
Manufacturer	OMG (0x3DA7)
Ident number	12345678
Version	51
Date and time of read out	24.06.2020 09:45
Battery life	100 month

AES Key
= manu. spec. at least 8 bytes unique for each meter
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

AES CBC Initial Vector (LSB first):
= M Field + A Field + 8 bytes Access No
= A7 3D 78 56 34 12 33 03 01 01 01 01 01 01 01 01

Mioty Network Key According to FIPS 197 (see [OMS-S2] 9.1):
= manufacturer specific random key
= 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0 00

Mioty Nonce (Initial Vector) for AES-CTR according to FIPS 197 (LSB first):
= End Point EUI64 + 00h + DIR (1B) + Packet Counter (4B) + Block Counter (2B)
= 00 12 4B 00 1C BC E3 32 00 DIR 00 00 00 0n 00 00

Note: DIR = 00h for uplink, 01h for downlink
Note: SND-IR use Packet Counter = 00 00 00 01
Note: CNF-IR use Packet Counter = 00 00 00 01 (value from last uplink packet)

Mioty Nonce (Initial Vector) for SIGN according to FIPS 197 (LSB first):
= End Point EUI64 + 00h + DIR (1B) + Packet Counter (4B) + FFFFh
= 00 12 4B 00 1C BC E3 32 00 DIR 00 00 00 0n FF FF

Note: Same as for AES-CTR encryption except 0xFFFF is used instead of Block counter

A.3 SND-IR

Table A.3 – SND-IR

Byte No		OMS wM-Bus frame over mioty	OMS end-device -> mioty Base Station			Layer
	Field Name	Content	Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	
1	MAC Header	MPF present, rx open			48h	MAC
2	Address	Short Address (16 bit) (=ACDCh)			ACh	MAC
3	Address				DCh	MAC
4	MPDUCNT	MPDUCNT (24 bit) (=000001h)			00h	MAC
5	MPDUCNT				00h	MAC
6	MPDUCNT				01h	MAC
7	MPF	MAC Payload Format field		83h	0Dh	MAC
8	MBAL-CL	MBAL Control field		16h	D8h	MBAL
9	CI	CI-Field		72h	1Dh	Transport Layer (TPL)
10	ID	Identification number (LSB)		78h	D7h	Transport Layer (TPL)
11	ID	Identification number		56h	C1h	Transport Layer (TPL)
12	ID	Identification number		34h	00h	Transport Layer (TPL)
13	ID	Identification number (MSB)		12h	67h	Transport Layer (TPL)
14	MF	Manufacturer (LSB)		A7h	A7h	Transport Layer (TPL)
15	MF	Manufacturer (MSB)		3Dh	07h	Transport Layer (TPL)
16	DV	Device version		33h	6Fh	Transport Layer (TPL)
17	DT	Device type		03h	DDh	Transport Layer (TPL)
18	ACC	Access number (TPL)		01h	49h	Transport Layer (TPL)
19	STS	Status		00h	C7h	Transport Layer (TPL)
20	CF	Configuration field (LSB)		18h	38h	Transport Layer (TPL)
21	CF	Configuration field (MSB)		05h	F8h	Transport Layer (TPL)
22	AES-Verify	Decryption verification	2Fh	EDh	54h	Transport Layer (TPL)
23	AES-Verify	Decryption verification	2Fh	A8h	12h	Transport Layer (TPL)
24	DR1 DIF	Curr. date/time	04h	FEh	45h	Application Layer (APL)
25	DR1 VIF	Curr. date/time	6Dh	D5h	7Bh	Application Layer (APL)
26	DR1 Value	Curr. date/time	2Dh	AAh	2Ah	Application Layer (APL)
27	DR1 Value	Curr. date/time	09h	FDh	DBh	Application Layer (APL)
28	DR1 Value	Curr. date/time	98h	6Ah	BBh	Application Layer (APL)
29	DR1 Value	Curr. date/time	26h	96h	59h	Application Layer (APL)
30	DR2 DIF	Battery life time in month	01h	F6h	32h	Application Layer (APL)
31	DR2 VIF	Battery life time in month	FDh	8Ah	64h	Application Layer (APL)
32	DR2 VIFE	Battery life time in month	FDh	7Fh	59h	Application Layer (APL)
33	DR2 VIFE	Battery life time in month	02h	ACh	04h	Application Layer (APL)
34	DR2 Value	Battery life time in month	64h	CAh	F1h	Application Layer (APL)
35	Dummy	Fill Byte due to AES	2Fh	86h	BEh	Application Layer (APL)
36	Dummy	Fill Byte due to AES	2Fh	74h	FBh	Application Layer (APL)
37	Dummy	Fill Byte due to AES	2Fh	F7h	16h	Application Layer (APL)
38	SIGN	CMAC (32 bit)			ACh	MAC
39	SIGN				05h	MAC
40	SIGN				A5h	MAC
41	SIGN				F7h	MAC

A.4 CNF-IR

Table A.4 – CNF-IR

Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	Layer
		OMS wM-Bus frame over mioty	mioty Base Station -> OMS end-device			
1	MAC Header	MPF present			40h	MAC
2	MPF	MAC Payload Format field		83h	4Ch	
3	MBAL-CL	MBAL Control field		36h	2Bh	MBAL
4	CI	CI-Field		80h	D8h	TPL
5	ID	Identification number (LSB)		78h	F5h	
6	ID	Identification number		56h	ADh	
7	ID	Identification number		34h	62h	
8	ID	Identification number (MSB)		12h	BEh	
9	MF	Manufacturer (LSB)		A7h	21h	
10	MF	Manufacturer (MSB)		3Dh	2Eh	
11	DV	Device version		33h	10h	
12	DT	Device type		03h	6Fh	
13	ACC	Access number (TPL)		01h	4Eh	
14	STS	Status		00h	88h	
15	CF	Configuration field (LSB)		00h	C6h	
16	CF	Configuration field (MSB)		00h	D4h	
17	SIGN	CMAC (32 bit)			7Dh	MAC
18	SIGN				EFh	
19	SIGN				94h	
20	SIGN				5Ch	

A.5 General Parameters

Table A.5 – General parameters

Gas meter example	
Medium	Gas
Manufacturer	OMG (0x3DA7)
Ident number	12345678
Version	21
Forward absolute meter volume, temperature converted	28504,27 m³
Date and time of read out	31.05.2008 23:50
Error code binary	0

Individual Master Key Mk
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Current Message Counter C (LSB first)
= B3 0A 00 00

Encryption Session Key Kenc
= CMAC(Mk, 0x00 || MCR || Ident No || padding)
= CMAC(Mk,00||B3||0A||00||00||78||56||34||12 …
... ||07||07||07||07||07||07||07)
= EC CF 39 D4 75 D7 30 B8 28 4F DF DC 19 95 D5 2F

MAC Session Key Kmac
= CMAC(Mk, 0x01 || MCR || Ident No || padding)
= CMAC(Mk,01||B3||0A||00||00||78||56||34||12 …
... ||07||07||07||07||07||07||07)
= C9 CD 19 FF 5A 9A AD 5A 6B BD A1 3B D2 C4 C7 AD

Mioty Network Key According to FIPS 197 (see [OMS-S2] 9.1):
= manufacturer specific random key
= 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0 00

Mioty Nonce (Initial Vector) for AES-CTR according to FIPS 197 (LSB first):
= End Point EUI64 + 00h + DIR (1B) + Packet Counter (4B) + Block Counter (2B)
= 00 12 4B 00 1C BC E3 32 00 00 00 00 00 01 00 00

Mioty Nonce (Initial Vector) for SIGN according to FIPS 197 (LSB first):
= End Point EUI64 + 00h + DIR (1B) + Packet Counter (4B) + FFFFh

= 00 12 4B 00 1C BC E3 32 00 DIR 00 00 00 01 FF FF

A.6 SND-NR

Table A.6 – SND-NR

Byte No	Field Name	Content	OMS end-device -> mioty Base Station Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	Layer
		OMS wM-Bus frame over mioty				
1	MAC Header	MPF present, rx open			48h	MAC
2	Address	Short Address (16 bit) (=ACDCh)			ACh	
3	Address				DCh	
4	MPDUCNT	MPDUCNT (24 bit) (=000001h)			00h	
5	MPDUCNT				00h	
6	MPDUCNT				01h	
7	MPF	MAC Payload Format field		83h	0Dh	
8	MBAL-CL	Control field (limited access, SND-NR)		14h	DAh	MBAL
9	CI Field	Authentication and Fragmentation layer		90h	FFh	AFL
10	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	A0h	
11	FCL	Fragmentation Control Field (LSB)		00h	97h	
12	FCL	Fragmentation Control Field (MSB)		2Ch	18h	
13	MCL	Message Control Field		25h	50h	
14	MCR	Message Counter C (LSB)		B3h	B3h	
15	MCR	Message Counter C (e.g.=2739)		0Ah	30h	
16	MCR	Message Counter C (e.g.=AB3h)		00h	5Ch	
17	MCR	Message Counter C (MSB)		00h	DEh	
18	MAC	AES-CMAC (MSB)		21h	69h	
19	MAC	AES-CMAC		92h	55h	
20	MAC	AES-CMAC		4Dh	6Dh	
21	MAC	AES-CMAC		4Fh	B2h	
22	MAC	AES-CMAC		2Fh	96h	
23	MAC	AES-CMAC		B6h	0Ch	
24	MAC	AES-CMAC		6Eh	D5h	
25	MAC	AES-CMAC (LSB)		01h	AFh	
26	CI	CI-Field		7Ah	FAh	TPL
27	ACC	Access number (TPL)		75h	53h	
28	STS	Status		00h	D1h	
29	CF	Configuration field (LSB)		20h	EFh	
30	CF	Configuration field (MSB)		07h	C3h	
31	CFE	Confiugration field extension		10h	FEh	
32	AES-Verify	Decryption verification	2Fh	90h	B6h	
33	AES-Verify	Decryption verification	2Fh	58h	F0h	
34	DR1 DIF	Curr. meter reading	0Ch	47h	7Ch	APL
35	DR1 VIF	Curr. meter reading	14h	5Fh	67h	
36	DR1 Value	Curr. meter reading	27h	4Bh	C4h	
37	DR1 Value	Curr. meter reading	04h	C9h	28h	
38	DR1 Value	Curr. meter reading	85h	1Dh	95h	
39	DR1 Value	Curr. meter reading	02h	F8h	88h	
40	DR2 DIF	Curr. date/time	04h	78h	3Ch	

41	DR2 VIF	Curr. date/time	6Dh	B8h	B3h	
42	DR2 Value	Curr. date/time	32h	0Ah	B6h	
43	DR2 Value	Curr. date/time	37h	1Bh	7Ch	
44	DR2 Value	Curr. date/time	1Fh	0Fh	02h	
45	DR2 Value	Curr. date/time	15h	98h	61h	
46	DR3 DIF	Curr. status	02h	B6h	0Ch	
47	DR3 VIF	Curr. status	FDh	29h	0Dh	
48	DR3 VIFE	Curr. status	17h	02h	74h	
49	DR3 Value	Curr. status	00h	4Ah	28h	
50	DR3 Value	Curr. status	00h	ACh	D3h	
51	Dummy	Fill Byte due to AES	2Fh	72h	ACh	
52	Dummy	Fill Byte due to AES	2Fh	79h	38h	
53	Dummy	Fill Byte due to AES	2Fh	42h	DDh	
54	Dummy	Fill Byte due to AES	2Fh	BFh	9Eh	
55	Dummy	Fill Byte due to AES	2Fh	C5h	C9h	
56	Dummy	Fill Byte due to AES	2Fh	49h	BCh	
57	Dummy	Fill Byte due to AES	2Fh	23h	BAh	
58	Dummy	Fill Byte due to AES	2Fh	3Ch	41h	
59	Dummy	Fill Byte due to AES	2Fh	01h	73h	
60	Dummy	Fill Byte due to AES	2Fh	40h	F4h	
61	Dummy	Fill Byte due to AES	2Fh	82h	ADh	
62	Dummy	Fill Byte due to AES	2Fh	9Bh	E2h	
63	Dummy	Fill Byte due to AES	2Fh	93h	EEh	
64	SIGN	CMAC (32 bit)			A5h	MAC
65	SIGN				25h	
66	SIGN				70h	
67	SIGN				27h	

A.7 General Parameters

Table A.7 – General parameters

Water meter example	
Medium	Water (07h)
Manufacturer	OMG (0x3DA7)
Ident number (M-Bus)	12345678
Version	01

M-Bus Application AES Key According to FIPS 197 (see 9.1):
= manu. spec. at least 8 bytes unique for each meter
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

M-Bus AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + Version + Device Type + 8 bytes Access No
= A7 3D 78 56 34 12 01 07 A3 A3 A3 A3 A3 A3 A3 A3

Mioty Network Key According to FIPS 197 (see [OMS-S2] 9.1):
= manufacturer specific random key
= 10 20 30 40 50 60 70 80 90 A0 B0 C0 D0 E0 F0 00

Mioty Nonce (Initial Vector) for AES-CTR according to FIPS 197 (LSB first):
= End Point EUI64 + 00h + DIR (1B) + Packet Counter (4B) + Block Counter (2B)
= 00 12 4B 00 1C BC E3 32 00 DIR 00 00 00 0n 00 00

Note: DIR = 00h for uplink, 01h for downlink

Note: SND-UD(2) use Packet Counter = 00 00 00 01 (value from last uplink packet)

Note: ACK, RSP-UD use Packet Counter = 00 00 00 02 (incremented counter)

Mioty Nonce (Initial Vector) for SIGN according to FIPS 197 (LSB first):
= End Point EUI64 + 00h + DIR (1B) + Packet Counter (4B) + FFFFh
= 00 12 4B 00 1C BC E3 32 00 DIR 00 00 00 0n FF FF

Note: Same as for AES-CTR encryption except 0xFFFF is used instead of Block counter

A.8 SND-UD Correction of Time

Table A.8 – SND-UD Correction of time

Byte No		OMS wM-Bus frame over mioty	mioty Base Station -> OMS end-device			Layer
	Field Name	Content	Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	
1	MAC Header	MPF present, resp. exp., rx open, prio			5Ch	MAC
2	MPF	MAC Payload Format field		83h	4Ch	
3	MBAL-CL	MBAL Control field		22h	3Fh	MBAL
4	CI	CI-Field		6Dh	35h	TPL
5	ID	Identification number (LSB)		78h	F5h	
6	ID	Identification number		56h	ADh	
7	ID	Identification number		34h	62h	
8	ID	Identification number (MSB)		12h	BEh	
9	MF	Manufacturer (LSB)		A7h	21h	
10	MF	Manufacturer (MSB)		3Dh	2Eh	
11	DV	Device version		01h	22h	
12	DT	Device type		07h	6Bh	
13	ACC	Access number (TPL)		A3h	ECh	
14	STS	Status		00h	88h	
15	CF	Configuration field (LSB)		10h	D6h	
16	CF	Configuration field (MSB)		05h	D1h	
17	AES-Verify	Decryption verification	2Fh	91h	91h	
18	AES-Verify	Decryption verification	2Fh	C2h	65h	
19	TC-Field	Add time difference	01h	5Ch	CAh	APL
20	Time	Value format J, LSB	32h	60h	D0h	
21	Time	Value (add 50 seconds)	00h	DEh	58h	
22	Time	Value MSB	00h	13h	71h	
23	Reserved	Reserved, set to 0	00h	CBh	79h	
24	Reserved	Reserved, set to 0	00h	DCh	B6h	
25	Reserved	Reserved, set to 0	00h	6Ah	C7h	
26	Reserved	Reserved, set to 0	00h	A9h	55h	
27	Reserved	Reserved, set to 0	00h	C4h	8Dh	
28	Reserved	Reserved, set to 0	00h	78h	59h	
29	CMD-Verify	Command verification	2Fh	78h	BCh	
30	CMD-Verify	Command verification	2Fh	C8h	BFh	
31	CMD-Verify	Command verification	2Fh	70h	1Ch	
32	CMD-Verify	Command verification	2Fh	56h	67h	
33	SIGN	CMAC (32 bit)			7Eh	MAC
34	SIGN				BAh	
35	SIGN				28h	
36	SIGN				93h	

A.9 ACK

Table A.9 – ACK

Byte No		OMS wM-Bus frame over mioty	OMS end-device -> mioty Base Station			Layer
	Field Name	Content	Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	
1	MAC Header	MPF present, rx open, ack			49h	MAC
2	Address	Short Address (16 bit) (=ACDCh)			ACh	
3	Address				DCh	
4	MPDUCNT	MPDUCNT (24 bit) (=000002h)			00h	
5	MPDUCNT				00h	
6	MPDUCNT				02h	
7	MPF	MAC Payload Format field		83h	CDh	
8	MBAL-CL	MBAL Control field		10h	11h	MBAL
9	CI	CI-Field		7Ah	E9h	TPL
10	ACC	Access number (TPL)		A3h	57h	
11	STS	Status		00h	F4h	
12	CF	Configuration field (LSB)		00h	E4h	
13	CF	Configuration field (MSB)		00h	68h	
14	SIGN	CMAC (32 bit)			B4h	MAC
15	SIGN				88h	
16	SIGN				39h	
17	SIGN				76h	

A.10 SND-UD2 Correction of Time

Table A.10 – SND-UD2 Correction of time

Byte No		OMS wM-Bus frame over mioty	mioty Base Station -> OMS end-device			Layer
	Field Name	Content	Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	
1	MAC Header	MPF present, resp. exp., rx open, prio			5Ch	MAC
2	MPF	MAC Payload Format field		83h	4Ch	
3	MBAL-CL	MBAL Control field		23h	3Eh	MBAL
4	CI	CI-Field		6Dh	35h	TPL
5	ID	Identification number (LSB)		78h	F5h	
6	ID	Identification number		56h	ADh	
7	ID	Identification number		34h	62h	
8	ID	Identification number (MSB)		12h	BEh	
9	MF	Manufacturer (LSB)		A7h	21h	
10	MF	Manufacturer (MSB)		3Dh	2Eh	
11	DV	Device version		01h	22h	
12	DT	Device type		07h	6Bh	
13	ACC	Access number (TPL)		A3h	ECh	
14	STS	Status		00h	88h	
15	CF	Configuration field (LSB)		10h	D6h	
16	CF	Configuration field (MSB)		05h	D1h	
17	AES-Verify	Decryption verification	2Fh	91h	91h	
18	AES-Verify	Decryption verification	2Fh	C2h	65h	
19	TC-Field	Add time difference	01h	5Ch	CAh	APL
20	Time	Value format J, LSB	32h	60h	D0h	
21	Time	Value (add 50 seconds)	00h	DEh	58h	
22	Time	Value MSB	00h	13h	71h	
23	Reserved	Reserved, set to 0	00h	CBh	79h	
24	Reserved	Reserved, set to 0	00h	DCh	B6h	
25	Reserved	Reserved, set to 0	00h	6Ah	C7h	
26	Reserved	Reserved, set to 0	00h	A9h	55h	
27	Reserved	Reserved, set to 0	00h	C4h	8Dh	
28	Reserved	Reserved, set to 0	00h	78h	59h	
29	CMD-Verify	Command verification	2Fh	78h	BCh	
30	CMD-Verify	Command verification	2Fh	C8h	BFh	
31	CMD-Verify	Command verification	2Fh	70h	1Ch	
32	CMD-Verify	Command verification	2Fh	56h	67h	
33	SIGN	CMAC (32 bit)			70h	MAC
34	SIGN				49h	
35	SIGN				3Bh	
36	SIGN				23h	

A.11 RSP-UD Empty Response

Table A.11 – RSP-UD Empty response

Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] M-Bus encr	Bytes [hex] mioty encr	Layer
		OMS wM-Bus frame over mioty	OMS end-device -> mioty Base Station			
1	MAC Header	MPF present, rx open, ack			49h	MAC
2	Address	Short Address (16 bit) (=ACDCh)			ACh	
3	Address				DCh	
4	MPDUCNT	MPDUCNT (24 bit) (=000002h)			00h	
5	MPDUCNT				00h	
6	MPDUCNT				02h	
7	MPF	MAC Payload Format field		83h	CDh	
8	MBAL-CL	MBAL Control field		18h	19h	MBAL
9	CI	CI-Field		7Ah	E9h	TPL
10	ACC	Access number (TPL)		A3h	57h	
11	STS	Status		00h	F4h	
12	CF	Configuration field (LSB)		00h	E4h	
13	CF	Configuration field (MSB)		00h	68h	
14	DR1	Idle Filler		2Fh	8Ah	APL
15	SIGN	CMAC (32 bit)			EFh	MAC
16	SIGN				BFh	
17	SIGN				3Fh	
18	SIGN				B0h	