Open Metering System
Technical Report 06
OMS over LoRaWAN

Version 2.0.8 – 2022-12
RELEASE

Document History

- V 0.0.1: Initial template
- V 0.0.2: Results of editing in meeting #5
- V 0.0.3: Contributions and modifications by A. Kasttet
- V 0.0.4: Results of editing in meeting #6
- V 0.0.5: Contributions and modifications by A. Kasttet and Uwe Pahl as per the Meeting Minutes #6
  - Addition of LoRaWAN specifications references
  - Addition of figures and tables numbers and legends
  - Update of the Layer Structure according to [EN 13757-7]
  - Details of LoRaWAN's addressing and activation procedure
  - Separation of the Architecture Figure in to figures one for data exchange and another for the activation and key distribution
- V 0.0.6: Modifications according to meeting #7
  - Change of Document's structure according to M. Pahl recommendations
  - Update of Figure 1 and Figure 2 and the corresponding descriptions
  - Addition of new entries in the Glossary table
  - Renaming of Section "Security Key distribution" to "Security Information Exchange"
  - Moving Paragraph "Data Rate Adaptation" to section 6 in addition ADR bit usage clarification
  - Addition of Paragraph 4.3 "relation between LoRaWAN and M-Bus address
  - Addition of Annex B: "LoRaWAN Meta Data"
  - Addition of an introductive summary to section 3.1
  - Feeding of MAC services section
  - Addition of an introductive text to 6.1. "Types of messages" section
  - Shall, may and should in Capital letters as per LoRaWAN spec conventions
- V 0.0.7: Technical changes:
  - Document revision live during Meeting#8
  - Addition of Chapter 7 on Security
  - Content of Annex B placed in § 6.4
- V 0.0.8: Editorial and format changes
- V 0.0.9: Modification during meeting #10:
  - Introduction of a new chapter for the role of the Application Server
  - New FPort mechanism for OMS over LoRaWAN
  - End to End Description of installation sequence
  - Deinstallation of an OMS end-device description with multiple scenarios
  - Additional Security overhead by security profile and impact on Payload size description (see action item #9-1)
  - New table for the chapter "Type of Messages"
  - OMS over LoRaWAN examples
- V 0.1.0: Editorial changes:
  - Alignment of column widths, font and coloring in all tables
  - Table headlines and numbering in Annex A
  - Integration of Excel tables in Annex A
- V0.1.1: Editorial changes:
  - Add OED, TPL, and wM-Bus terms in the glossary
  - Introduce OED term to refer to OMS end-device
  - Systematically use dash (-) for OMS end-device
  - Use headline shaping when referring to sections in the text
  - Add OMS to when referring to security profile
  - Use lower case for SHOULD when it is used for "it should be noted"
- V1.0.0: Release candidate

  Technical changes:
  - FPorts in Table 3 changed
  - Headline of 5.3 changed
  - Table 9 was revised
  - FPort assignments in tables in Annex A updated

  Editorial changes:
  - Abbreviation OED and dash for "OMS End Device" removed
  - Lower case for "SHALL"/"SHOULD"/"MAY"
  - Column widths of tables in Annex A optimized
  - Drawing of tables in Annex A corrected
  - New table numbering for Annex A
  - Alignment of capitalization for headlines of chapters, tables and figures

- V1.0.1: Release candidate
  Technical and editorial changes:
  - Integration of comments from OMS internal review
  - Editorial changes for the sake of consistency (OMS End Device, AMMHES, …)
  - Consistent and more detailed Installation Sequence figure
  - Adding Reference to [LA TS-002 1.1.0] where relevant
- V1.0.2: Release candidate
- V1.0.3: Release
  Technical and editorial changes:
  - Add "OMS over " before LoRaWAN in the Header title
  - Remove filename from the footer
  - Remove break page between pages 19 and 20
  - Replace "Link Layer Error" by "M-Bus Rejection” in Table 3 for NACK message name
  - Replace "Repetitions" by "Transmissions" in table 7
  - Reshape Examples tables to remove some blue colors and display issues
  - Tables 2, 3, 5, 7 and 9 corrected
  - Wording and spelling correction
- V2.0.0 to 2.0.5: Draft
  - Alignment with last draft of [prEN13757-8] with regards to MBAL usage
  - Update of FPort values reserved for OMS
  - Update of Table 4: Type of Messages
  - Update of Figure 4: Installation sequence
  - Update of Table 1: General Layer Structure
- V2.0.6: Release candidate
  - Copyright remark added to front page
- V2.0.7: Release candidate
  Technical and editorial changes:
  - Integration of submitted comments
- V2.0.8: Release
  Technical and editorial changes:
  - Chapter 6.1.6 added
  - Table 10 completed
  - Alignment of term “OMS end-device”

Contents

Document History 2
Contents 4
Tables 5
Figures 5
1 Introduction 6
1.1 Preface 6
1.2 General 6
1.3 Glossary of Terms 7
1.4 References 10
2 General Layer Structure 11
2.1 Overview 11
2.2 M-Bus Application over LoRaWAN 11
3 Overview of LoRaWAN's Architecture 12
3.1 Network Architecture 12
3.1.1 Overview of the Network Architecture 12
3.1.2 Data Exchange 12
3.1.3 Security Information Exchange 12
3.1.4 Role of the Application Server 13
3.2 Ownership of Servers 13
4 Address of the OMS End-device 14
4.1 LoRaWAN Address 14
4.2 M-Bus Address 14
4.3 Relation between LoRaWAN Address and M-Bus Address 14
5 Installation / Deinstallation of an OMS End-device 16
5.1 States of a LoRaWAN End Device 16
5.2 Installation Procedure 16
5.3 Changing the Status of an OMS End-device 18
6 Data Exchange 19
6.1 OMS over LoRaWAN using MBAL 19
6.1.1 Overview 19
6.1.2 MBAL Version 19
6.1.3 OMS End-device Accessibility 19
6.1.4 OMS End-device Latency 19
6.1.5 Type of Messages 19
6.1.6 Fragmented Messages 20
6.2 MAC Services 20
6.3 Data Rate Adaptation 21
6.4 Meta Data to be provided to the Application Server 21
6.4.1 LoRaWAN Meta Data Overview 21
6.4.2 Device Identification and Frame Content 21
6.4.3 Frame Type 21
6.4.4 Uplink Packet RF Meta Data 21
6.4.5 OMS End-device Configuration 22

6.5 Message Content of an OMS End-device (refer to OMS-S2 Annex B) 22
7 Security Mechanisms 23
7.1 Security Mechanisms Overview 23
7.2 LoRaWAN Security 23
7.3 Additional Security by M-Bus 23
7.4 Security versus Packet Size and Data Rate 24
Annex A (informative): 25
OMS Over LoRaWAN Frame Examples 25
A.1 Overview Table 25
A.2 General Parameters 26
A.3 Installation Request 28
A.4 Installation Confirm 30
A.5 Application Data Up with OMS Security Profile A 31
A.6 Application Data Up with OMS Security Profile B and AFL 33
A.7 Application Data Down with ASP10 and AFL 36

Tables

Table 1 - OMS over LoRaWAN general layers structure 11
Table 2 - States of a LoRaWAN device on the NS level 16
Table 3 - MBAL-CL Field Structure Overview 19
Table 4 - LoRaWAN and Wireless M-Bus messages correspondence 20
Table 5 - LoRaWAN packet content and identification 21
Table 6 - LoRaWAN frame type 21
Table 7 - LoRaWAN RX frame RF meta data 22
Table 8 - OMS end-device configuration on LoRaWAN Network 22
Table 9 - Additional TPL security for OMS end-device 23
Table 10 - Additional security overhead by security profiles 24

Figures

Figure 1 - OMS over LoRaWAN data exchange 12
Figure 2 - OMS over LoRaWAN end-device activation and key exchange 13
Figure 3 - Relation between LoRaWAN and M-Bus addresses 15
Figure 4 - Installation sequence of an OMS end-device over LoRaWAN 17

1 Introduction

1.1 Preface

This document describes the requirements for a combined layer structure with LoRaWAN and M-Bus. It was created in a joint task force with members of OMS Group and the LoRa Alliance.

The specifications and standardizations in this document enable the development of interoperable solutions combining the advantages of M-Bus and LoRaWAN.

1.2 General

The [EN 13757] “Communication Systems for Meters” Standard series covers several communication layers including the application layer. It can be transported both over wired and wireless links.

LoRaWAN is a wireless communication protocol, dedicated for battery powered devices, that could be used by an application to exchange data with a communication partner.

This document proposes an architecture to transport [EN 13757] “higher layers” over the LoRaWAN physical and link layer using the Adaptation layer mechanism defined in [prEN13757-8]. The overall architecture of this mechanism is depicted in Table 1.

1.3 Glossary of Terms

Additional terms and clarifications for glossary annex of [OMS-S1] (see chapter 4 for reference).

Term	Description
A	**A**
ABP	Activation by Personalization
AppKey	Application Key
AppSKey	Application Session Key: AES 128 Key material used to encrypt and / or De-encrypt LoRaWAN application payload.
AS	Application Server: Entity receiving and / or transmitting data from and / to the OMS end-devices through a LoRaWAN network.
ASP	Application Security Profile
B	**B**
C	**C**
CI-Field	Control Information Field, contains the type of command sent (set baud rate, application reset, select slave, etc.)
D	**D**
DL	Downlink
Downlink	LoRaWAN Packet sent from the Network Server to the OMS end-device
DR	Data Rate: Speed of signal modulation.
E	**E**
End-device	In this TR, an end-device communicating over LoRaWAN according to [LA TS001 1.0.4].
ED	End-device
F	**F**
FCnt	Frame Counter
FCtrl	Frame Control Octet
FHDR	Frame Header: LoRaWAN Mac Header added on top of the payload.
FOpts	Frame Options
FPort	Frame Port: LoRaWAN header field used by the application to differentiate payloads.
FRMPayload	Frame payload
FType	Frame Type: Type of the LoRaWAN frame.
G	**G**
Gateway	LoRaWAN's Network infrastructure element relaying packets between the NS and OMS end-devices

H	**H**
HES	Head End System
I	**I**
J	**J**
JS	Join Server according to [LA TS001 1.0.4].
K	**K**
L	**L**
LSB	Least Significant Byte
M	**M**
MAC	Media Access Control (used for radio layer 2 in LoRaWAN)
MAC	Message Authentication Code (in the context of security)
Master	Provides the power on the M-Bus. Collects data from the slave devices on the M-Bus.
MBAL	M-Bus Adaptation Layer
Message	Refer to the application data that an OMS end-device exchange with an AS and vice versa, on which overhead, of low layers, is added according to the communication protocol. A message could be sent in one or more payloads.
MHDR	MAC Header
MIC	Message Integrity Code
MSB	Most Significant Byte
N	**N**
NwkSKey	Network Session Key: AES 128 Key material used to authenticate, encrypt and check the integrity of LoRaWAN packets
NS	Network Server: Entity responsible of managing the network connectivity of the OMS end-devices
O	**O**
OMS end-device	A meter/actuator, radio adapter or sensor, according to OMS definition, that implements this TR recommendations. The term OMS end-device in this TR is used for devices using LoRaWAN-communication and not wired or wireless M-Bus.
OED	OMS end-device
OTAA	Over-the-air activation
P	**P**
Packet	A LoRaWAN packet is the whole sequence of bytes that is transmitted over the air. It consists of the concatenation of the payload, the intermediate layers contents, the LoRaWAN header and control fields.
Payload	Application data sent or received by the communication protocol. One or more payloads form a Message.

Q	**Q**
R	**R**
REQ-UD1	The master Requests User Data (class 1)
REQ-UD2	The master Requests User Data (class 2)
RFU	Reserved for Future Use
RSP-UD	Response with user data
S	**S**
SND-NKE	The value of the FCB is adjusted in master and slave and the slave is deselected when secondary addressing is used
SND-UD	Send User Data to slave
SP_x	Defines the Security Profile x according to [OMS-S2], clause 9
T	**T**
U	**U**
Uplink	A LoRaWAN Packet sent from the OMS end-device to the Network Server
User	A person who designs, installs or starts up M-Bus installations in the field.
V	**V**
W	**W**
wM-Bus	Wireless M-Bus
X	**X**
Y	**Y**
Z	**Z**

1.4 References

OMS References:

- [OMS-S1]: OMS Specification Volume 1, General Part, Issue 2.3.1
- [OMS-S1], Annex A: Appendix to the OMS Specification Volume 1, Glossary of Terms, Issue 2.3.1
- [OMS-S2]: OMS Specification Volume 2, Primary Communication, Issue 4.5.1
- [OMS-CTS] OMS-Conformance-Test-Specification 4.0 Release 6, Volume 1 General Part, Issue 4.0.8, Volume 2 PHY (Radio Parameters), Issue 4.0.11, Volume 3 Data Link Layer, Issue 4.0.8, Volume 4 Application layer, Issue 4.0.12

EN standards:

- [EN 13757-3]: Communication systems for meters – Part 3: Application protocols; August 2018 is currently valid. All references are linked to the standard edition of August 2018 unless a date is specified.
- [EN 13757-7]: Communication systems for meters – Part 7: Transport and security services; first edition August 2018
- [EN 13757-4]: Communication systems for meters – Part 4: Wireless M-Bus communication; May 2019
- [prEN 13757-8] : Communication systems for meters – Part 8: Adaptation Layer; 2021
- [CEN/TR 17167] Communication system for meters – Accompanying TR to [EN 13757-2], [EN 13757-3] and [EN 13757-7], Examples and supplementary information
- [EN 60870-5-2]: Telecontrol equipment and systems – Part 5: Transmission Protocols – Part 2: Link transmission procedures, EN 60870-5-2:1992

LoRa Alliance:

- LoRaWAN L2 1.0.4 Specification [LA TS001 - 1.0.4]
- LoRaWAN Regional Parameters [LA RP002 - 1.0.1]
- LoRaWAN_Certification_Protocol_v1.0.0 [LA TS009 - v1.0.0]
- LoRaWAN Back End Interfaces [LA TS002 – 1.1.0]

Further set of rules:

- M-Bus documentation: “The M-Bus: A Documentation” Rev. 4.8 from www.M-Bus.com
- Technical Directive BSI TR-03109-1, Requirements for the interoperability of the communication unit of an intelligent measuring system, version 1.1

2 General Layer Structure

2.1 Overview

This document proposes an architecture to transport [EN 13757] “higher layers” over the LoRaWAN physical and link layer following the specification of the M-Bus Adaptation Layer (MBAL) given in [prEN 13757-8]. The general layer structure of this mechanism is depicted in Table 1.

A valid LoRaWAN packet contains at least the link layer elements as described in [LA TS001 – 1.0.4]. The application, transport and the authentication and fragmentation layers, if present, are introduced by specific CI-field values as explained in [EN 13757-7]. The usage of the “higher layers” (APL, TPL, and AFL) shall comply with [EN 13757] standard and OMS specifications rules. The MBAL is inserted between the M-Bus “higher layers” and the LoRaWAN layers.

Table 1 - OMS over LoRaWAN general layers structure

<table>
<tr><th>OSI Model
Layers</th><th>M-Bus
Layers</th><th>[EN 13757]
Related Parts</th><th>OMS Over LoRaWAN
Layers</th></tr>
<tr><td>Application
Presentation</td><td>Application Layer (APL)</td><td>[EN 13757-3]</td><td>APL</td></tr>
<tr><td rowspan="2">Session
Transport</td><td>Transport Layer (TPL)</td><td>[EN 13757-7]</td><td>TPL</td></tr>
<tr><td>Authentication and
Fragmentation (AFL)</td><td>[EN 13757-7]</td><td>AFL</td></tr>
<tr><td>[Adaptation Layer]</td><td>Adaptation Layer (MBAL)</td><td>[prEN 13757-8]</td><td>MBAL</td></tr>
<tr><td>Network [a]</td><td>Network Layer (NWL) [a]</td><td>[EN 13757-5] [a]</td><td rowspan="4">LoRaWAN</td></tr>
<tr><td rowspan="2">Data Link (LLC/MAC)</td><td>Extended Link Layer (ELL)</td><td rowspan="3">[EN 13757-4]</td></tr>
<tr><td>Data Link Layer (DLL)</td></tr>
<tr><td>Physical</td><td>Physical Layer (PHY)</td></tr>
<tr><td colspan="4">[a] Network Layer is not implemented in OMS Specification</td></tr>
</table>

2.2 M-Bus Application over LoRaWAN

An OMS end-device is potentially able to run multiple applications on top of LoRaWAN. In order to segregate these multiple applications traffic, a specific field of LoRaWAN L2, called FPort (Frame Port), according to [LA TS001 - 1.0.4], is used. The M-Bus protocol relies on the CI-Field to introduce the Transport and Application Layers.

In order to transport M-Bus over LoRaWAN those two mechanisms (FPort and CI-Field) will be used in conjunction according to the scheme defined in [prEN 13757-8], Annex D. On one hand, the CI-Field principle will remain the same according to [OMS-S2], 2.2. On the other hand, FPort will be used to transport the MBALCL field (as described in 6.1) and signal that a LoRaWAN packet, in both Uplink and Downlink directions, carries M-Bus application messages according to this document. If the LoRaWAN packet is carrying a different type of application message, it shall use a different FPort value from the dedicated values 112 to 223 as stated in §4.3.2 of [LA TS001 - 1.0.4]. The FPort range 2 to 111 is reserved for OMS-conform transmissions (See 6.1.5, Table 4). FPort value 1 is reserved for future use of OMS over LoRaWAN.

3 Overview of LoRaWAN's Architecture

3.1 Network Architecture

3.1.1 Overview of the Network Architecture

LoRaWAN networks features multiple entities that exchange two types of information:

- Data exchange: This consists on transporting, in both directions, application messages and network signaling information.
- Security information exchange: This consists on the establishment of the security context and the exchange of key materials between network elements to enable security services during data exchange.

3.1.2 Data Exchange

LoRaWAN networks are composed of End Devices using Radio Frequency link to communicate with gateways. A packet from the End Device (Uplink) could be received by one or several gateways, while a packet to the End Device could be transmitted only by one gateway at a given time. The End Devices and the gateways are managed by a central entity running at the backend called the Network Server (NS). An End Device sends, via the NS, its application data message to a remote counterpart called the Application Server (AS) and vice versa. Data exchange on LoRaWAN networks is depicted on Figure 1.

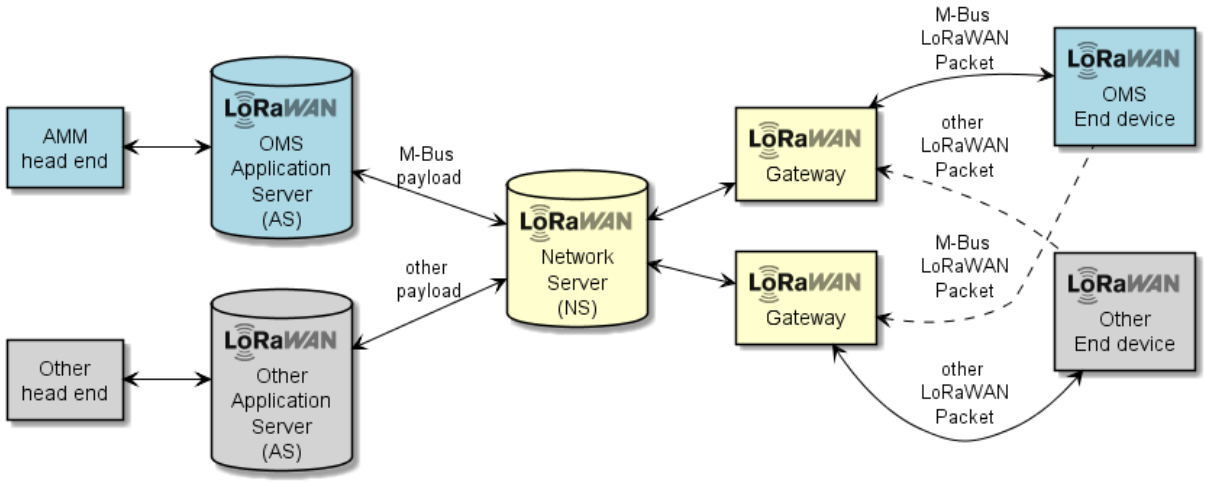

Figure 1 - OMS over LoRaWAN data exchange

3.1.3 Security Information Exchange

The Join Server (JS) is a key management system responsible of the key derivation and distribution between all the previous entities during the Over The Air Activation (OTAA) also called "Join Procedure" of an OMS End Device. In order to successfully connect to a LoRaWAN network, an End Device shall be firstly provisioned in the NS and JS data base. After receiving the Join-Request packet from a provisioned End Device, the NS will forward it to the JS. The JS will proceed to the authentication and the key derivation mechanisms as described in [LA TS001 - 1.0.4 §6.2]. The JS will then provide the NwkSKey to the NS and AppSKey to the AS. The OTAA's steps, depicted in Figure 2, could be summarized as:

1. The manufacturer stores the AppKey, JoinEUI and DevEUI in the OMS end-device and forward them securely to the JS.
2. The AS provisions the device in NS (DevEUI and JoinEUI)
3. The OMS end-device triggers the Transmission of a Join Request packet.
4. The NS forwards it (JoinReq) to the JS which authenticates the JoinReq (based on AppKey and DevEUI), derivates AppSkey and NwkSKey and generate the JoinAccept.
5. JS forwards the AppSkey to AS
6. JS forwards the NwkSkey to NS
7. JS forwards the JoinAccept to NS
8. NS forwards JoinAccept to OMS end-device
9. OMS end-device authenticates and decrypts the JoinAccept and then derives NwkSkey and AppSkey

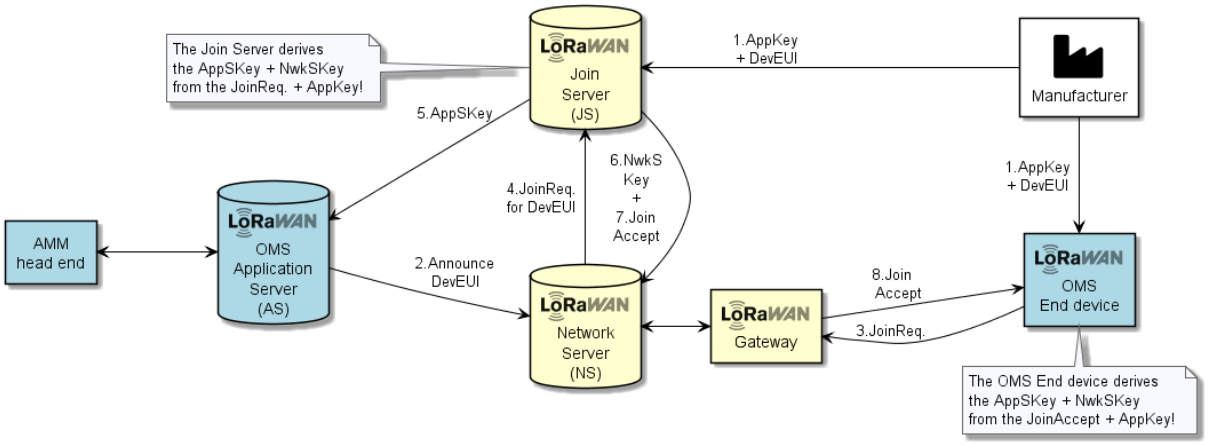

Figure 2 - OMS over LoRaWAN end-device activation and key exchange

3.1.4 Role of the Application Server

The Application Server (AS) is a key element of the architecture as it plays the role of interface between the LoRaWAN Network Server (NS) and the AMM Head End System (HES). The AS will receive LoRaWAN payloads from the NS that it will forward to the AMMHES, and it will receive payloads from the AMMHES that will be transferred to the OMS end-device through the NS. As it owns the AppSKey (See 7.2), the Application Server is also responsible of decrypting (in Uplink) and encrypting (in Downlink) the payloads.

As an OMS end-device is able to run multiple applications in parallel, the AS is also responsible of routing the payloads to the appropriate HES or any other server depending on DevEUI (see 4.1) and the FPort (See 2.2). During the provisioning process (Step 2 in 3.1.3), i.e. during the declaration of an OMS end-device in the NS, every DevEUI is tied to the appropriate AS who knows which applications are supported for this DevEUI and the corresponding FPort. When the AS receive the payload, it checks if the DevEUI of this OMS end-device is stored in its database. If yes, it uses the FPort and DevEUI to forward this payload to the corresponding HES. A set of FPort numbers for M-Bus messages types are defined in 6.1.

3.2 Ownership of Servers

The Network Server is typically owned by the network operator while the Application Server is owned by the service provider or the OMS end-device manufacturer. The Join Server could be operated either by the service provider, the network operator, or a Trusted Third Party. The network infrastructure including gateways is managed by the network operator.

4 Address of the OMS End-device

4.1 LoRaWAN Address

Any OMS end-device intended to be connected to a LoRaWAN network shall have a unique 8 bytes identifier called DevEUI (End Device EUI as per [LA TS001 - 1.0.4 §6.2.1]) corresponding to an IEEE (Extended Unique Identifier) EUI64 address (also known as MAC address). In that 8 bytes space, an OUI (Organization Unique Identifier) is assigned by the IEEE RA (Registration Authority) using 3 options (MA-L: 24 bits, MA-M: 28 bits or MA-S: 36 bits). The usage of a MA-L is recommended for OMS.

In order to exchange data with the AS via the NS, the OMS end-device shall have an OMS end-device address (DevAddr), a network session key (NwkSKey) and an application session key (AppSKey). This triplet of security materials is obtained after the so-called Activation procedure [LA TS001 - 1.0.4 §6.1]. There are two ways in LoRaWAN to activate an End Device:

- Over The Air Activation (OTAA): As described in 3.1.3, the triplet of security material is obtained over the air via the NS and the JS following the Join procedure [LA TS001 - 1.0.4 §6.2].
- Activation By Personalization (ABP): {DevAddr, NwkSKey, AppSKey} are pre-stored in the OMS end-device's memory and shared with the NS and AS out of band [LA TS001 - 1.0.4 §6.3].

As the ABP mechanism does not allow the revocation or change of the security material triplet if needed, an OMS over LoRaWAN OMS end-device shall not use ABP and shall use the OTAA mechanism instead.

After receiving a Join-Request from a provisioned OMS end-device, the NS will allocate (in the Join-Accept message) a 32 bits address DevAddr (that identifies that OMS end-device within the current network) as specified in [LA TS001 - 1.0.4 §6.1.1]. All the subsequent messages (Uplink and Downlink) will use the DevAddr as the identifier of the device. It should be noted that this DevAddr may vary after each new Join procedure. The DevEUI is transmitted by the OMS end-device only during the Join Procedure as described in [LA TS001 - 1.0.4 §6.2].

4.2 M-Bus Address

According to the general layer structure adopted in this document, the protocol stack will use the LoRaWAN's link layer as specified in [LA TS001 - 1.0.4]. Therefore, the Link Layer Address (LLA) as stated in [OMS-S2] will not be present in band. The OMS end-device shall use the DevEUI and the DevAddr according to [LA TS001 - 1.0.4]. However, the Application Layer Address (ALA) according to [OMS-S2] shall be present at least in the first Uplink, following the reception of the Join-Accept, using the M-Bus long header format as described in the installation procedure in 5.2.

4.3 Relation between LoRaWAN Address and M-Bus Address

The DevEUI and the DevAddr are used to identify the OMS end-device within the LoRaWAN Network. The DevEUI is unique whereas the DevAddr may be changed by the NS after each new Join procedure. The M-Bus Address defines the metering application (including the device type) of the metering device. This address is essential to identify the metering point.

As long as the relation between DevEUI and M-Bus address is one to one, it is sufficient if the M-Bus address is transmitted in the Installation Request message (according to 5.2). If the relation between DevEUI and M-Bus address is one to many (e.g. a LoRaWAN-adapter hosting more than one M-Bus device) then the M-Bus address shall be transmitted in uplink and downlink within each message.

The transmission of a LoRaWAN packet with M-Bus address requires the use of a TPL long header (according to [OMS-S2], Table 1) whereas the transmission without M-Bus Address allows the use of the TPL short header format.

For a clear identification of the metering device, the Application Server shall store the following information for each connected OMS end-device:

- DevEUI
- M-Bus address

When the Application Server forwards the M-Bus payload from an OMS end-device to the AMMHES, it shall use the M-Bus address as identifier.

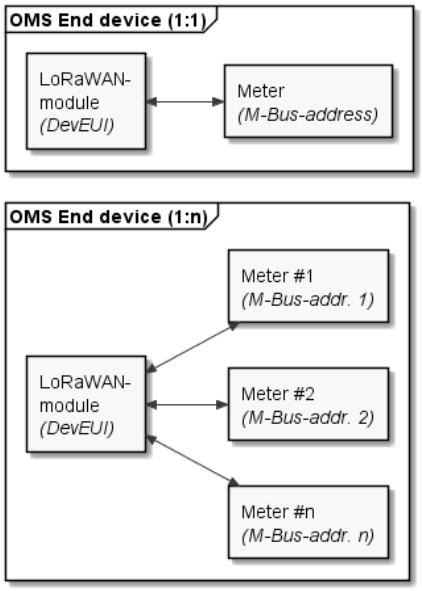

Figure 3 - Relation between LoRaWAN and M-Bus addresses

5 Installation / Deinstallation of an OMS End-device

5.1 States of a LoRaWAN End Device

From the NS perspective, an OMS end-device may be in one of the states described in Table 2.

Table 2 - States of a LoRaWAN device on the NS level

Device Status	Description
Provisioned	The OMS end-device DevEUI is declared in the Join Server's and the Network Server Data Bases. The NS is waiting for a Join-Request message.
Joining	JoinRequest Received, Join-Accept sent and the NS is waiting for the first uplink
Connected	First Uplink successfully received
Error	NS is receiving invalid datagrams (MIC Error, …)
Deprovisioned	Device is deprovisioned from JS / NS Data Base.

5.2 Installation Procedure

After successfully joining the LoRaWAN (i.e. receiving a valid Join Accept at the end of the Over The Air Activation procedure described in section 3.1.3), the OMS end-device shall periodically transmit an Installation Request message , acting as a "SND-IR", on the OMS Over LoRaWAN dedicated FPort (described in 6.1) using the long TPL header format until it receives an application message in downlink, Installation Confirm, acting as "CNF-IR" from the OMS HES. The usage of long TPL header format is mandatory for the Installation Request to establish the mapping between M-Bus address and DevEUI at the AS level as described in 4.3. This roundtrip communication signals that an end-to-end connection has successfully been established between the OMS end-device and the AMMHES. This also validates the OMS end-device's security context (LoRaWAN payloads have been successfully authenticated and decrypted/encrypted) and ensure that the AS has correctly forwarded the Uplink and the M-Bus address to the AMMHES based on DevEUI and FPort.

In this way, the AS and the AMMHES can use the M-Bus address to identify each OMS end-device. The AS is responsible of translating this M-Bus address to DevEUI and vice versa.

During this installation phase, it is not necessary to use the Confirmed Data Up Frame Type as the OMS end-device is trying to validate its connection on the application layer level not on the link layer level (which has been validated at the end of the Join Procedure).

This sequence is represented in the Figure 4.

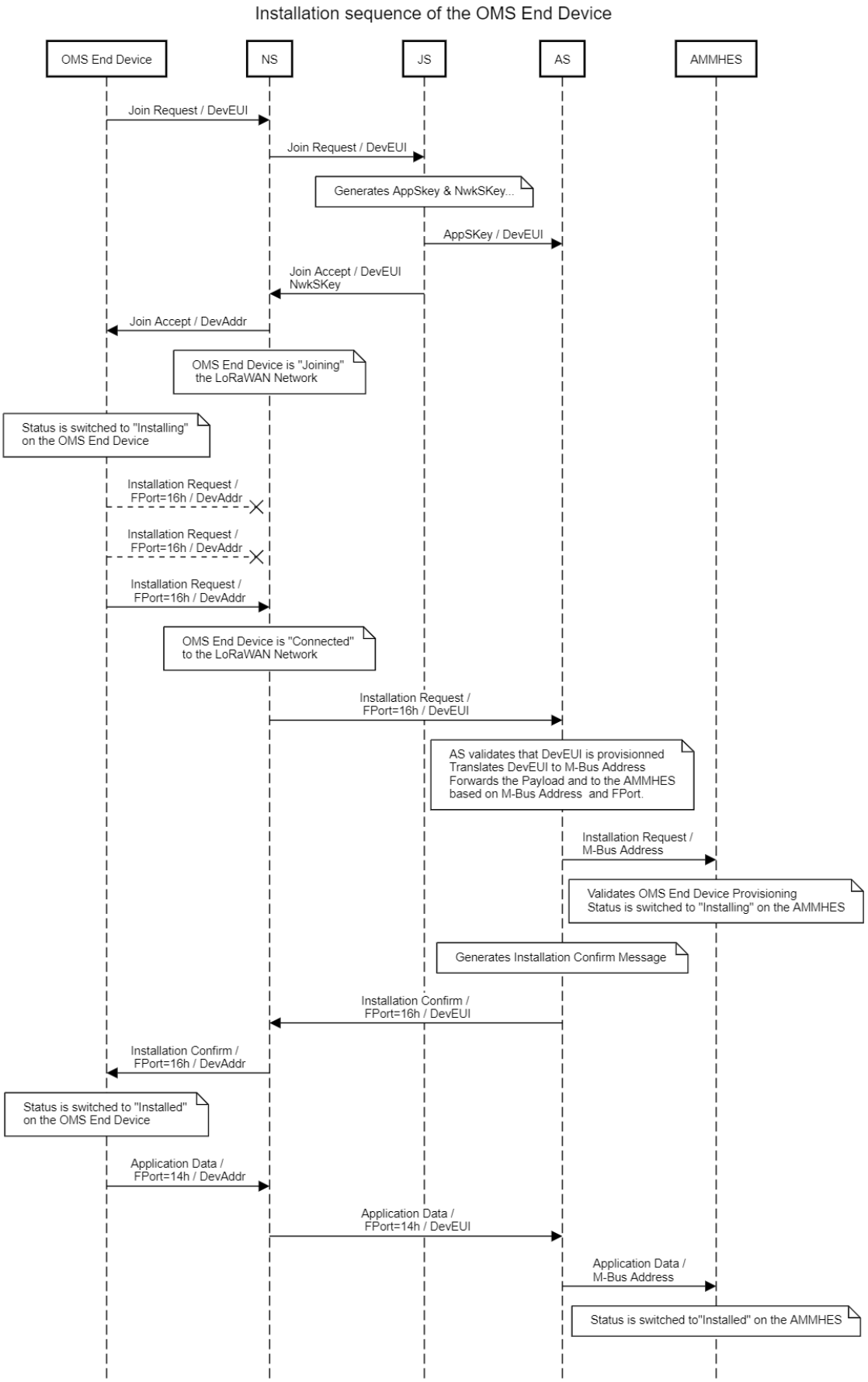

Figure 4 - Installation sequence of an OMS end-device over LoRaWAN

5.3 Changing the Status of an OMS End-device

During the life cycle of the OMS end-device, the application or service provider may decide to:

1. Deinstall the OMS end-device from the AMMHES

   Once the OMS end-device is deinstalled (i.e. removed) from the AMMHES, its packets could not be processed any more. It is recommended to notify the application layer of the OMS end-device via the AS, prior to the deinstallation, to stop transmissions if this removal is permanent. Alternatively, the AS could decide to route the traffic to a different HES providing that the necessary security material is transferred to the new HES.

2. Disconnect the OMS end-device from the LoRaWAN network

   When the OMS end-device is deprovisioned from the NS (see 5.1), all the packets coming from and going to this OMS end-device will be dropped by the NS. It is recommended to order the OMS end-device, via application layer, to stop any LoRaWAN traffic once this disconnection is effective. Alternatively, the OMS end-device may restart the join procedure.

3. Change OMS end-device's current LoRaWAN network

   In order to change the current NS of an OMS end-device, it is necessary to disconnect it, as described above, and provision it in the new NS. To connect to this new NS, the OMS end-device shall send a Join Request and receive a Join Accept (see 3.1.3 and 4.1). In the LoRaWAN 1.0.x, there is no way for the network (i.e., using MAC commands) to force the OMS end-device to send a Join Request message. This should be managed by the application server or any other specific tool (which is out of the scope of this document). This scenario is equivalent to "Roaming". For more details on Roaming between multiple LoRaWAN Networks, see [LA TS002 – 1.1.0].

4. Renew the security key material

   If the application layer aims to renew the LoRaWAN security material, the OMS end-device shall restart a Join Procedure as described in 3.1.3.

6 Data Exchange

6.1 OMS over LoRaWAN using MBAL

6.1.1 Overview

The OMS over LoRaWAN scheme defined on this document relies in the Adaptation layer mechanism described in Annex D of [prEN 13757-8]. In this case, there is no need for a specific CI Field to introduce the MBAL. Thus, the MBAL is compact and composed of the 1 byte MBAL-Control Field which will be placed in the FPort. The MBALCL structure as described in Table 4 and Table 5 of [prEN 13757-8] is depicted in Table 3:

Table 3 - MBAL-CL Field Structure Overview

Bits		[7..6]	[5..4]	[3..0]
MBAL-CL	**Downlink**	Version	Latency	Function Code
	Uplink	Version	Access	Function Code

6.1.2 MBAL Version

According to [prEN 13757-8], Table 8, MBAL Version 1 (value 00b) is used.

6.1.3 OMS End-device Accessibility

Depending on the class of operation, LoRaWAN supports both Accessibility value 1 (01b) for Class A & B and value 2 (10b) for Class C as described the mapping table given in Table D.4 of [prEN 13757-8], Annex D.

(00b) can be used in unsolicited messages from the OMS end-device to signal that the OMS end-device application is currently unable to process commands.

If the OMS end-device application is not able to process the HES command, it should use the Application Busy information in the Status byte of the TPL in the response transmitted to the HES.

The accessibility information provided by the MBAL-CL field should be used instead of that provided by the Configuration field (Bits A & B) of the TPL which should be ignored.

6.1.4 OMS End-device Latency

The latency is dictated by the OMS Application Server when sending a DL to the end-device. Whether the end-device should delay its response or send it immediately is application specific and depends on duty cycle limitations and power consumption constraints of each use case. As stated in [prEN 13757-8], Table 10, when the OMS Application Server expects a fast response from the OMS end-device, it should use Latency value 10b. Alternatively, when no response is requested or when the answer could be sent at the OMS end-device discretion, latency value 01b should be used.

6.1.5 Type of Messages

As the OMS end-devices will be connected to LoRaWAN networks, M-Bus link layer will not be used and will be replaced by LoRaWAN as stated in chapter 2.1. The LoRaWAN protocol offers confirmed and unconfirmed frames in both directions (Uplink and Downlink). The Frame Type field of LoRaWAN's MAC header allows the selection of "Confirmed" or "Unconfirmed" packets by the application depending on its type of services. A "Confirmed" LoRaWAN packet expects an answer from the counterpart (ED in Downlink and NS in Uplink) setting the ACK bit in the FCtrl field.

The usage of Confirmed or Unconfirmed communication mechanisms when transporting application payloads remains at the discretion of the application or the link layer. The OMS end-device should use an unconfirmed frame as default mode. The Acknowledgement field used in the LoRaWAN header simply validates the successful reception by the link layer (See [prEN 13757-8], Annex D, D.6.2.2).

To keep the same message flow scheme as M-Bus, the function code of each M-Bus message will be encoded in the FPort field.

The correspondence between wM-Bus message types and the applicable FPort number is given in the following Table 4 assuming:

- Class A or Class B (Access subfield = 01b) or Class C (Access subfield = 10b)
- Response to downlinks sent with delay (Latency subfield = 01b) or sent as soon as possible (Latency subfield = 10b)
- In case the M-Bus application is not able to accept messages after the unsolicited transmission, the Access subfield = 00b is used.

The expected response when receiving one of the following messages is given in [prEN 13757-8], Table 11 and Table 12.

Table 4 - LoRaWAN and Wireless M-Bus messages correspondence

Service	Direction	FPort[c]	Symbolic Name	Function Code of MBAL-CL [a]
Installation Request	Up	06h, 16h, 26h	SND-IR	6h
Installation Confirm	Down	16h, 26h	CNF-IR	6h
Application data [d]	Up/Down	04h, 14h, 24h	SND-NR	4h
Additional Access slot to OMS end-device	Up	07h, 17h, 27h	ACC-NR	7h
Alarm Indication	Up	0Ah, 1Ah, 2Ah	ACC-DMD	Ah
Alarm Indication compact sequence	Up	05h, 15h, 25h	ACC-DMD2	5h
Alarm request	Down	1Ah, 2Ah	REQ-UD1	Ah
Data request	Down	1Bh, 2Bh	REQ-UD2	Bh
Data Send and expect ACK	Up/Down	02h, 12h, 22h	SND-UD	2h
Data Send and expect response	Down	13h, 23h	SND-UD2	3h
Link Reset	Down	17h, 27h	SND-NKE	7h
Response to Data Request	Up	18h, 28h	RSP-UD	8h
M-Bus Rejection	Up/Down	11h, 21h	TPL-NACK[b]	1h
M-Bus Acknowledgement	Up/Down	10h, 20h	TPL-ACK	0h

[a] According to [prEN 13757-8], 7.2.1.5

[b] May be applied in case of memory buffer overflow or invalid FPort number

[c] In the uplink, FPort shall be 0xh if no access to application is available, 1xh for class A or B operation, and 2xh for class C operation. In the downlink, FPort shall be 1xh to request a reply with normal delay, and 2xh for the fast reply (low latency) where x refers to the Function Code.

[d] Application data contains either a standard data message (with consumption data) or a static message (with management data). The messages types shall be separated in the configuration field according to OMS-S2, 7.2.4.6. Table 22.

6.1.6 Fragmented Messages

In case of a fragmented message, LoRaWAN confirmed uplinks or downlinks shall be used (see 6.4.3 and §4.2.1.2 of [LA TS001 - 1.0.4]). The subsequent fragment shall be transmitted after receiving the confirmation for the reception of the previous fragment.

The OMS end-device is responsible for the management of the fragmentation session in the uplink direction. The AMMHES is responsible for the management of the fragmentation session in the downlink direction.

6.2 MAC Services

In order to optimize LoRaWAN's OMS end-devices and networks operation, a set of MAC commands are available. They can be sent either by the OMS end-device or the NS. These MAC commands enable the modification and the setting of multiple RF parameters such as Data Rate (DR), Duty Cycle, EIRP, Channels Frequencies, etc.…

Each MAC command has an identifier and few bytes of a specific content (possibly empty). It could be transmitted either along with an application message in the FOpts field or separately in a LoRaWAN packet using FPort 0. It should be noted that a sequence of MAC commands could be sent in a single LoRaWAN packet. For more details, see Chapter 5 of [LA TS001 - 1.0.4].

6.3 Data Rate Adaptation

The LoRaWAN Physical layer features several data rates usable by an OMS end-device. When receiving uplink messages, the NS is able to estimate the most suitable data rate for a device depending on the link quality to optimize battery consumption and network capacity. In order to enable this feature, the OMS end-device shall set the bit ADR (Adaptive Data Rate) in the FCtrl field of “LoRaWAN Frame Header” (FHDR) according to §4.3.1.1 of [LA TS001 - 1.0.4]. The setting of this bit is mandatory for OMS end-devices.

If an OMS end-device requires a higher DR (to carry bigger payload in a single packet) than what it has been allocated by the NS, it shall unset the ADR bit. In that case, the packet is no longer expected to be delivered to the NS, as the link budget of the new DR will be lower than the previous one. Hence, the OMS end-device will be no longer compliant with this OMS recommendation.

6.4 Meta Data to be provided to the Application Server

6.4.1 LoRaWAN Meta Data Overview

LoRaWAN Packets received/transmitted by the NS contain several Meta Data such as RF parameters, Timestamp, etc... The following sections provide examples of information that could be exchanged between the NS and the AS. It should be noted that the interfaces, the content and the periodicity of these exchanges have to be negotiated between the Application provider and network operator and are out of the scope of this document. The NS-NS and NS-JS interfaces are specified in [LA TS002 – 1.1.0].

6.4.2 Device Identification and Frame Content

A LoRaWAN packet received/transmitted by the NS, carry the information given in the following Table 5.

Table 5 - LoRaWAN packet content and identification

Field	DevAddr	DevEUI	FCnt	FPort	FRMPayload
Size (Bytes)	4	8	4	1	0-242

6.4.3 Frame Type

For each LoRaWAN packet received on the NS, the Frame Type could be provided. According to §4.2.1 of [LA TS001 - 1.0.4], Frame Type field values are shown in Table 6.

Table 6 - LoRaWAN frame type

FType (Binary)	Description
000	Join Request
001	Join Accept
010	Unconfirmed Data Up
011	Unconfirmed Data Down
100	Confirmed Data Up
101	Confirmed Data Down
110	RFU
111	Proprietary

6.4.4 Uplink Packet RF Meta Data

For each LoRaWAN packet received by the NS and delivered to the AS, the following Meta Data may be provided to a dedicated server via an appropriate interface as shown in Table 7. More information could be found in Chapter 17 of [LA TS002 – 1.1.0].

Table 7 - LoRaWAN RX frame RF meta data

Meta data	Symbol	Unit
Gateway count	GwCnt	NA
Data Rate	DR	[0-7]
Received Signal Strength Indication	RSSI	dBm
Signal to Noise Ratio	SNR	dB
UL Frequency	ULFreq	*100 Hz

6.4.5 OMS End-device Configuration

For each OMS end-device, the following information may be provided by the NS to a dedicated server belonging to the application provider using an appropriate interface and periodicity (see Table 8). More information could be found in Chapter 18 of [LA TS002 – 1.1.0].

Table 8 - OMS end-device configuration on LoRaWAN Network

OMS end-device parameter	Symbol	Size (Bytes)	Description
End-device Equipment Unique Identifier	DevEUI	8	IEEE Device Identifier
End-device Address	DevAddr	4	Device Identifier on the NS
Channel Mask	ChMask	2	Mask of active Channels
Data Rate Range/ Channel	DRRange	1*3 – 1*16	List of DR range with one byte per active channel.
TX Power	TxPower	1	Current Tx Power [2-14] (dBm)
Number of Transmissions	NbTrans	1	Number of Uplink Transmissions [1-15]
Data Rate	DR	1	Current DR [0-7]
Max Duty Cycle	MaxDCycle	1	Configured Max DC [1-15]
Rx Delay	RxDelay	1	RX Window Delay [1-15] (Seconds)
RX1 Data Rate Offset	RX1DROffset	1	Offset between TX & RX1 DR. [0-5]
RX2 Frequency	RX2Freq	3	*100 Hz
RX2 Data Rate	RX2DR	1	Current RX2 DR

6.5 Message Content of an OMS End-device (refer to OMS-S2 Annex B)

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

7 Security Mechanisms

7.1 Security Mechanisms Overview

Every OMS end-device willing to use a LoRaWAN network shall comply with the LoRaWAN security mechanisms specified in [LA TS001 - 1.0.4]. Every LoRaWAN packet is end-to-end encrypted, origin authenticated, and integrity protected. An application running using LoRaWAN protocol is free to add supplementary security mechanisms (See **7.3**), on top of LoRaWAN's security scheme. This comes at the expense of a higher overhead and therefore leading to an additional power consumption and spectrum occupancy.

7.2 LoRaWAN Security

The key exchange mechanism described in section 3.1.3 enables the LoRaWAN protocol to ensure the following security properties:

- Mutual Authentication: Thanks to the Join Procedure, the JS and the OMS end-device (owning the same AES 128 Root Key AppKey) are ensured to authenticate each other and to share the same security material (NwkSkey and AppSkey). This confirms that only authorized OMS end-device communicate with authentic LoRaWAN Network. For more details, see [LA TS001 - 1.0.4 §6.2].
- Integrity and origin authentication: Every LoRaWAN packet exchanged on the network carry a MIC (Message Integrity Code). This 4 bytes AES-CMAC field calculated using the NwkSkey, guarantee that the LoRaWAN packet has not been tampered during transmission and enables the receiver to prove the authenticity of the packet. The MIC is described in [LA TS001 - 1.0.4 §4.4].
- End to End Confidentiality: The FRMPayload of every LoRaWAN packet is encrypted using an AES-CTR algorithm as explained in [LA TS001 - 1.0.4 §4.3.3]. The usage of AppSKey for the encryption ensures an end to end confidentiality between the AS and the OMS end-device. The NS cannot eavesdrop application messages as it does not own the AppSkey.
- Replay protection: A Frame Counter (one for Uplink and another for Downlink) is contained in the Frame Header of each LoRaWAN packet (See [LA TS001 - 1.0.4 §4.3.1.5]). It is incremented for each new application payload. The Frame Counter is part of the MIC calculation. It enables the receiver, which keeps track of the value, to detect replayed packets.

7.3 Additional Security by M-Bus

Any OMS end-device may use M-Bus TPL security services according to its application needs. The possible OMS security profiles are defined in [OMS-S2], Table 36 as follow:

Table 9 - Additional TPL security for OMS end-device

OMS Security profile	Description	Support in OMS end-device
No Security profile	This profile has no security services. It relies on the security services provided by the LoRaWAN protocol as described above.	YES
Security Profile A	Provides additional encryption	YES
Security Profile B	Providing additional encryption and authentication	YES
Security Profile C	Applies a TLS session over LoRaWAN	YES (only if the data rate is sufficient) see (7.4)
Security Profile D	Providing additional encryption and authentication with lower overhead than security profile B	YES

An OMS end-device may use additional APL security according to [OMS-S2], 9.4.2, Table 40.

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

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

7.4 Security versus Packet Size and Data Rate

Depending on network coverage conditions, the NS selects a suitable DR for every OMS end-device. Hence, the maximum size of the FRMPayload may vary from 51 Bytes to 242 according to [LA RP002 - 1.0.1] for EU868 region. The usage of an additional M-Bus security profile will increase the size of the message to be transmitted. In the case of one packet per message, the available application payload size will be reduced depending on the selected security profile.

If no additional security demands are required, the use of “No Security Profile” allows maximum FRMPayload and minimize the packet size and hence optimize the power consumption and spectrum occupancy.

For high security demands, Security Profiles A, B or C defined in 7.3 should be selected (see Table 10).

Table 10 - Additional security overhead by security profiles

	Overhead size			**Payload size (FRMPayload)**		
Layer	SITP/TLS	AFL	TPL	FRMPayload	FRMPayload	FRMPayload
M-Bus APL				10	20	40
SP_0 (short TPL-Header)			5	15	25	45
SP_0 (long TPL-Header)			13	23	33	53
SP_A (short TPL-Header)			7	21	37	53
SP_A (long TPL-Header)			15	29	45	61
SP_B (short TPL-Header)		17	8	39	55	71
SP_B (long TPL-Header)		17	16	47	63	79
SP_C (long TPL-Header)	54		14	84	100	116
SP_D (short TPL-Header)			19	29	39	59
SP_D (long TPL-Header)			27	37	47	67
SP_0 (long TPL-Header) + ASP10	26		13	49	71	87

This table gives the resulting FRMPayload size for three APL messages (10, 20 and 40 Bytes) for different Security Profiles and TPL, AFL and ASP settings. It shows that the overhead could become rapidly significant especially for Security Profiles B, C and ASP10.

Depending on the current DR of the OMS end-device, the FRMPayload can be transported in one single LoRaWAN packet or in multiple packets using AFL when the FRMPayload size is limited for this DR (as stated in [LA RP002 - 1.0.1 §2.4.6]).

Annex A (informative):
OMS Over LoRaWAN Frame Examples

A.1 Overview Table

Table A.1 – List of examples

Example Name	Chapter	OMS Security Profile	Direction	FPort	Confirmed/ Unconfirmed	Counter
Installation Request	A.3	No	Up	16h	Unconfirmed	1
Installation Confirm	A.4	No	Down	16h	Unconfirmed	1
Application data up with sec. profile A	A.5	A	Up	14h	Unconfirmed	2
Application data up with sec. profile B and AFL	A.6	B	Up	14h	Unconfirmed	2, 3
Application data down with ASP10 and AFL	A.7	AFL+ASP	Down	13h	Unconfirmed	2, 3

A.2 General Parameters

Table A.2 – General parameters

LoraWAN example with water meter	
OMS end-device	
Device type	Water meter
Manufacturer	QDS (4493)
Ident number	12345678
Version	10
DevAddr	1A2B3C4D
NwkSKey	
= 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF	
AppSKey	
= 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46	
Individual Master Key MK (see [OMS-S2] 9.1):	
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	
Message Counter C_M (LSB first):	
= B3 0A 00 00	
Encryption Session Key Kenc	
= CMAC(Mk, 0x00 || MCR || IdentNo || 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 || IdentNo || 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

Application security key "Clock adjustment": (KeyID: 21h / KeyVersion: 00h)
= 08 15 47 11 08 15 47 11 08 15 47 11 08 15 47 11

Key counter for Application security (LSB first):
= 0F 00 00 00

A.3 Installation Request

Table A.3 – Installation request (no OMS security profile)

Byte No	OMS LoRaWAN frame		Water meter example			Layer
	Field Name	Content	Bytes [hex]		Bytes [hex]	
			plain		AES AppS Key)	
1	MHDR	MAC Header			40	MHDR
2	DevAddr	Device address (LSB)			4D	FHDR
3	DevAddr	Device address			3C	
4	DevAddr	Device address			2B	
5	DevAddr	Device address (MSB)			1A	
6	FCtrl	Frame control			80	
7	FCnt	Frame counter (LSB)			01	
8	FCnt	Frame counter (MSB)			00	
9	FPort	Frame Port			16	FPort
10	CI	CI-Field	72		9D	Transport Layer (TPL)
11	ID	Identification number (LSB)	78		9D	
12	ID	Identification number	56		06	
13	ID	Identification number	34		D9	
14	ID	Identification number (MSB)	12		FA	
15	MF	Manufacturer (LSB)	93		D6	
16	MF	Manufacturer (MSB)	44		3C	
17	DV	Device version	0A		CA	
18	DT	Device type	07		71	
19	ACC	Access number (TPL)	01		E8	
20	STS	Status	00		25	
21	CF	Configuration field (LSB)	08		02	
22	CF	Configuration field (MSB)	80		B1	
23	DR1 DIF	Curr. date/time	04		2F	Application Layer (APL)
24	DR1 VIF	Curr. date/time	6D		3A	
25	DR1 Value	Curr. date/time	2D		7F	
26	DR1 Value	Curr. date/time	09		C4	
27	DR1 Value	Curr. date/time	98		2E	
28	DR1 Value	Curr. date/time	26		6E	
29	DR2 DIF	Battery life time in month	01		DA	
30	DR2 VIF	Battery life time in month	FD		30	
31	DR2 VIFE	Battery life time in month	FD		D7	
32	DR2 VIFE	Battery life time in month	02		A7	
33	DR2 Value	Battery life time in month	64		F1	

34	DR3 DIF	Identification of the metering point	0C		B7	
35	DR3 VIF	Identification of the metering point	FD		79	
36	DR3 VIFE	Identification of the metering point	10		0A	
37	DR3 Value	Identification of the metering point	78		E7	
38	DR3 Value	Identification of the metering point	56		DE	
39	DR3 Value	Identification of the metering point	34		A0	
40	DR3 Value	Identification of the metering point	12		12	
41	MIC	Message integrity code			AA	MIC
42	MIC	Message integrity code			98	
43	MIC	Message integrity code			40	
44	MIC	Message integrity code			AB	

A.4 Installation Confirm

Table A.4 – Installation confirm (no OMS security profile)

Byte No	OMS LoRaWAN frame		Water meter example			Layer
	Field Name	Content	Bytes [hex]		Bytes [hex]	
			plain		AES (AppS Key)	
1	MHDR	MAC Header			60	MHDR
2	DevAddr	Device address (LSB)			4D	FHDR
3	DevAddr	Device address			3C	
4	DevAddr	Device address			2B	
5	DevAddr	Device address (MSB)			1A	
6	FCtrl	Frame control			80	
7	FCnt	Frame counter (LSB)			01	
8	FCnt	Frame counter (MSB)			00	
9	FPort	Frame Port			16	FPort
10	CI	CI-Field	80		F9	Transport Layer (TPL)
11	ID	Identification number (LSB)	78		75	
12	ID	Identification number	56		B3	
13	ID	Identification number	34		7C	
14	ID	Identification number (MSB)	12		52	
15	MF	Manufacturer (LSB)	93		BE	
16	MF	Manufacturer (MSB)	44		88	
17	DV	Device version	0A		8A	
18	DT	Device type	07		32	
19	ACC	Access number (TPL)	01		DC	
20	STS	Status	19		B1	
21	CF	Configuration field (LSB)	00		16	
22	CF	Configuration field (MSB)	C0		FF	
23	MIC	Message integrity code			8D	MIC
24	MIC	Message integrity code			5A	
25	MIC	Message integrity code			E8	
26	MIC	Message integrity code			E2	

A.5 Application Data Up with OMS Security Profile A

Table A.5 – Application data up with OMS Security Profile A

Byte No	OMS LoRaWAN frame		Water meter example			Layer	
	Field Name	Content	Bytes [hex]	Bytes [hex]	Bytes [hex]		
			plain	AES (MK)	AES (AppS Key)		
1	MHDR	MAC Header			40	MHDR	
2	DevAddr	Device address (LSB)			4D	FHDR	
3	DevAddr	Device address			3C		
4	DevAddr	Device address			2B		
5	DevAddr	Device address (MSB)			1A		
6	FCtrl	Frame control			80		
7	FCnt	Frame counter (LSB)			02		
8	FCnt	Frame counter (MSB)			00		
9	FPort	Frame Port			14	FPort	
10	CI	CI-Field		7A	D2	Transport Layer (TPL)	Application Layer (APL)
11	ACC	Access number (TPL)		02	F0		
12	STS	Status		00	8B		
13	CF	Configuration field (LSB)		20	F1		
14	CF	Configuration field (MSB)		85	F4		
15	DR0	Decryption verification	2F	B6	81		
16	DR0	Decryption verification	2F	49	F1		
17	DR1 DIF	Current Value	0C	17	47	#1	
18	DR1 VIF	Current Value	13	3E	1D		
19	DR1 Value	Current Value	89	11	27		
20	DR1 Value	Current Value	67	9E	CD		
21	DR1 Value	Current Value	45	5B	F0		
22	DR1 Value	Current Value	23	CE	6A		
23	DR2 DIF	Curr. date/time	04	CF	69		
24	DR2 VIF	Curr. date/time	6D	7F	7E		
25	DR2 Value	Curr. date/time	2D	FD	EA		
26	DR2 Value	Curr. date/time	09	0F	D7		
27	DR2 Value	Curr. date/time	98	CE	E4		
28	DR2 Value	Curr. date/time	26	EA	34		
29	DR3 DIF	Value at Due date	4C	FD	01		
30	DR3 VIF	Value at Due date	13	E6	3E		
31	DR3 Value	Value at Due date	78	CA	0D	#2	APL
32	DR3 Value	Value at Due date	56	D6	F1		
33	DR3 Value	Value at Due date	34	2F	ED		

34	DR3 Value	Value at Due date	12	F7	5B		
35	DR4 DIF	Due date	42	1E	DB		
36	DR4 VIF	Due date	6C	C0	13		
37	DR4 Value	Due date	7F	0B	10		
38	DR4 Value	Due date	2C	F9	78		
39	DR5	Fill bytes	2F	BF	1D		
40	DR5	Fill bytes	2F	78	EA		
41	DR5	Fill bytes	2F	0C	72		
42	DR5	Fill bytes	2F	AE	A5		
43	DR5	Fill bytes	2F	F4	A6		
44	DR5	Fill bytes	2F	5B	33		
45	DR5	Fill bytes	2F	F5	1A		
46	DR5	Fill bytes	2F	F3	1F		
47	MIC	Message integrity code			15	MIC	
48	MIC	Message integrity code			69		
49	MIC	Message integrity code			BC		
50	MIC	Message integrity code			2A		

A.6 Application Data Up with OMS Security Profile B and AFL

Table A.6 – Application data up with OMS Security Profile B and AFL Fragment #1

Byte No	OMS LoRaWAN frame		Water meter example			Layer
	Field Name	Content	Bytes [hex]	Bytes [hex]	Bytes [hex]	
			plain	AES (MK)	AES (AppS Key)	
1	MHDR	MAC Header			40	MHDR
2	DevAddr	Device address (LSB)			4D	FHDR
3	DevAddr	Device address			3C	
4	DevAddr	Device address			2B	
5	DevAddr	Device address (MSB)			1A	
6	FCtrl	Frame control			80	
7	FCnt	Frame counter (LSB)			02	
8	FCnt	Frame counter (MSB)			00	
9	FPort	Frame Port			14	FPort
10	CI	CI-Field		90	38	Authentication and Fragmentation Layer (AFL)
11	AFLL	AFL-length		09	FB	
12	FCL	Fragment control (LSB)		01	8A	
13	FCL	Fragment control (MSB)		78	A9	
14	MCL	Message control		65	14	
15	MCR	Message counter (LSB)		B3	84	
16	MCR	Message counter		0A	B2	
17	MCR	Message counter		00	50	
18	MCR	Message counter (MSB)		00	23	
19	ML	Message length (LSB)		26	10	
20	ML	Message length (MSB)		00	53	
21	CI	CI-Field		7A	D1	Transport Layer (TPL)
22	ACC	Access number (TPL)		02	A6	
23	STS	Status		00	A6	
24	CF	Configuration field (LSB)		20	21	
25	CF	Configuration field (MSB)		07	10	
26	CFE	Configuration field extension		10	C8	
27	DR0	Decryption verification	2F	F0	DA	
28	DR0	Decryption verification	2F	76	A8	
29	DR1 DIF	Current Value	0C	F3	0F	#1 ation Layer
30	DR1 VIF	Current Value	13	A6	7E	
31	DR1 Value	Current Value	89	81	46	
32	DR1 Value	Current Value	67	0C	2B	
33	DR1 Value	Current Value	45	58	9A	

34	DR1 Value	Current Value	23	0A	A6		
35	DR2 DIF	Curr. date/time	04	18	DD		
36	DR2 VIF	Curr. date/time	6D	30	E3		
37	DR2 Value	Curr. date/time	2D	6E	75		
38	DR2 Value	Curr. date/time	09	68	E9		
39	DR2 Value	Curr. date/time	98	28	8A		
40	DR2 Value	Curr. date/time	26	3F	AD		
41	DR3 DIF	Value at Due date	4C	0C	72		
42	DR3 VIF	Value at Due date	13	A9	A2		
43	DR3 Value	Value at Due date	78	70	22	#2	APL
44	DR3 Value	Value at Due date	56	FE	96		
45	DR3 Value	Value at Due date	34	94	7B		
46	DR3 Value	Value at Due date	12	73	9F		
47	DR4 DIF	Due date	42	C3	98		
48	DR4 VIF	Due date	6C	84	5F		
49	DR4 Value	Due date	7F	9F	C0		
50	DR4 Value	Due date	2C	AE	55		
51	DR5	Fill bytes	2F	5D	AD		
52	DR5	Fill bytes	2F	C1	18		
53	DR5	Fill bytes	2F	15	09		
54	DR5	Fill bytes	2F	AD	12		
55	DR5	Fill bytes	2F	DB	4A		
56	DR5	Fill bytes	2F	04	1C		
57	DR5	Fill bytes	2F	E3	04		
58	DR5	Fill bytes	2F	DF	45		
59	MIC	Message integrity code			B2	MIC	
60	MIC	Message integrity code			1E		
61	MIC	Message integrity code			A8		
62	MIC	Message integrity code			5D		

Table A.7 – Application data up with OMS Security Profile B and AFL Fragment #2

Byte No		OMS LoRaWAN frame	Water meter example			Layer
	Field Name	Content	Bytes [hex]	Bytes [hex]	Bytes [hex]	
			plain	AES (MK)	AES (AppS Key)	
1	MHDR	MAC Header			40	MHDR
2	DevAddr	Device address (LSB)			4D	FHDR
3	DevAddr	Device address			3C	
4	DevAddr	Device address			2B	
5	DevAddr	Device address (MSB)			1A	
6	FCtrl	Frame control			80	
7	FCnt	Frame counter (LSB)			03	
8	FCnt	Frame counter (MSB)			00	
9	FPort	Frame Port			14	FPort
10	CI	CI-Field		90	0F	Authentication and Fragmentation Layer (AFL)
11	AFLL	AFL-length		0A	9D	
12	FCL	Fragment control (LSB)		02	11	
13	FCL	Fragment control (MSB)		04	75	
14	MAC	AES-CMAC (MSB)		E2	90	
15	MAC	AES-CMAC		2C	33	
16	MAC	AES-CMAC		DA	26	
17	MAC	AES-CMAC		B9	35	
18	MAC	AES-CMAC		4E	36	
19	MAC	AES-CMAC		B5	9E	
20	MAC	AES-CMAC		7D	5A	
21	MAC	AES-CMAC (LSB)		CA	3B	
22	MIC	Message integrity code			37	MIC
23	MIC	Message integrity code			14	
24	MIC	Message integrity code			43	
25	MIC	Message integrity code			D4	

A.7 Application Data Down with ASP10 and AFL

Table A.8 – Application data down with ASP10 and AFL Fragment #1

Byte No	OMS LoRaWAN frame		Water meter example			Layer
	Field Name	Content	Bytes [hex]	Bytes [hex]	Bytes [hex]	
			plain	AES (ID= 21_h)	AES (AppS Key)	
1	MHDR	MAC Header			60	MHDR
2	DevAddr	Device address (LSB)			4D	FHDR
3	DevAddr	Device address			3C	
4	DevAddr	Device address			2B	
5	DevAddr	Device address (MSB)			1A	
6	FCtrl	Frame control			80	
7	FCnt	Frame counter (LSB)			02	
8	FCnt	Frame counter (MSB)			00	
9	FPort	Frame Port			13	FPort
10	CI	CI-Field		90	02	Authentication and Fragmentation Layer (AFL)
11	AFLL	AFL-length		05	66	
12	FCL	Fragment control (LSB)		01	0D	
13	FCL	Fragment control (MSB)		70	CA	
14	MCL	Message control		40	60	
15	ML	Message length (LSB)		35	8D	
16	ML	Message length (MSB)		00	BB	
17	CI	CI-Field		C3	CA	Transport Layer (TPL)
18	ID	Identification number (LSB)		78	3E	
19	ID	Identification number		56	09	
20	ID	Identification number		34	CC	
21	ID	Identification number (MSB)		12	F1	
22	MF	Manufacturer (LSB)		93	DB	
23	MF	Manufacturer (MSB)		44	AD	
24	DV	Device version		0A	B7	
25	DT	Device type		07	3E	
26	ACC	Access number (TPL)		31	E5	
27	STS	Status		00	35	
28	CF	Configuration field (LSB)		00	74	
29	CF	Configuration field (MSB)		C0	1D	
30	DR1 SITP	Block length	26	26	99	
31	DR1 SITP	Block length	00	00	7A	
32	DR2 SITP	Block ID field	00	00	B4	
33	DR3 SITP	Block control filed	20	20	36	

34	DR4 SITP	Recipient ID: No dedicated application	00	00	2E	Application Layer (APL)
35	DR5 SITP	DSI Auth. AES128-CMAC (8 Byte MAC)	32	32	CF	
36	DR6 SITP	Wrapper Key ID	21	21	81	
37	DR7 SITP	Wrapper Key Version	00	00	6C	
38	DR8 SITP	Key counter	0F	0F	B9	
39	DR8 SITP	Key counter	00	00	C7	
40	DR8 SITP	Key counter	00	00	B8	
41	DR8 SITP	Key counter	00	00	0C	
42	DR9 SITP	Target time	00	00	F2	
43	DR9 SITP	Target time	00	00	0D	
44	DR9 SITP	Target time	00	00	D9	
45	DR9 SITP	Target time	00	00	A3	
46	DR9 SITP	Target time	30	30	50	
47	DR10 SITP	Protocol ID: Time Sync	04	04	CF	
48	DR11 SITP	TC-Field (Add)	01	01	B2	
49	DR12 SITP	Correction value (Format J)	37	37	66	
50	DR12 SITP	Correction value (Format J)	00	00	12	
51	DR12 SITP	Correction value (Format J)	00	00	96	
52	DR13 SITP	Reserved bytes	00	00	45	
53	DR13 SITP	Reserved bytes	00	00	00	
54	DR13 SITP	Reserved bytes	00	00	CD	
55	DR13 SITP	Reserved bytes	00	00	B0	
56	DR13 SITP	Reserved bytes	00	00	D1	
57	DR13 SITP	Reserved bytes	00	00	38	
58	DR14 SITP	Command Verification	2F	2F	D5	
59	DR14 SITP	Command Verification	2F	2F	BD	
60	DR14 SITP	Command Verification	2F	2F	15	
61	MIC	Message integrity code			63	MIC
62	MIC	Message integrity code			CB	
63	MIC	Message integrity code			DD	
64	MIC	Message integrity code			91	

Table A.9 – Application data down with ASP10 and AFL Fragment #2

Byte No		OMS LoRaWAN frame	Water meter example			Layer
	Field Name	Content	Bytes [hex]	Bytes [hex]	Bytes [hex]	
			plain	AES (ID= 21_h)	AES (AppS Key)	
1	MHDR	MAC Header			60	MHDR
2	DevAddr	Device address (LSB)			4D	FHDR
3	DevAddr	Device address			3C	
4	DevAddr	Device address			2B	
5	DevAddr	Device address (MSB)			1A	
6	FCtrl	Frame control			80	
7	FCnt	Frame counter (LSB)			03	
8	FCnt	Frame counter (MSB)			00	
9	FPort	Frame Port			13	FPort
10	CI	CI-Field		90	A4	AFL
11	AFLL	AFL-length		02	08	
12	FCL	Fragment control (LSB)		02	1A	
13	FCL	Fragment control (MSB)		00	E6	
14	DR14 SITP	Command Verification		2F	53	APL
15	DR15 SITP	MAC		4E	36	
16	DR15 SITP	MAC		BA	D3	
17	DR15 SITP	MAC		27	43	
18	DR15 SITP	MAC		27	13	
19	DR15 SITP	MAC		E9	DB	
20	DR15 SITP	MAC		6D	77	
21	DR15 SITP	MAC		2F	31	
22	DR15 SITP	MAC		A2	67	
23	MIC	Message integrity code			B9	MIC
24	MIC	Message integrity code			A5	
25	MIC	Message integrity code			D5	
26	MIC	Message integrity code			4B	