P2 Companion Standard

Enexis Smart Meter Requirements

By order of:	**Enexis**
Date:	**2022, May 18th**
Version:	**ESMR 5.0, revision 5.9**
Status:	**Final**

CONTENTS

1 Introduction 5
1.1 Scope 5
1.2 System architecture 6
1.3 Normative references 7
1.4 Document structure 8
1.5 Document list 8

2 Physical Layer 9
2.1 Wireless connection 9

3 Data link layer 10
3.1 Wireless Connections 10
3.1.1 Length field (L) 10
3.1.2 Control field (C) 10
3.1.3 Manufacturer Identification field (MAN) 10
3.1.4 Address field (A: ID | VER | DEV) 11
3.1.5 Timing 11
3.1.5.1 Installation Mode 11
3.1.5.2 Regular hourly user data message 12
3.1.5.3 Regular 5 minutes user data message 12

4 Control Layer 13
4.1 Allowed control elements 13
4.2 Common control elements 16
4.2.1 Data Headers 16
4.2.2 Short Equipment Identifier (Short ID: ID | MAN | VER | DEV) 16
4.2.3 Version field 17
4.2.4 Access No. (ACC) 17
4.2.5 Status (ST) 17
4.2.6 Configuration word (CW) 17
4.3 Wireless Connections 17
4.3.1 Normalisation message 20
4.3.2 Hourly meter data message 21
4.3.3 5-min user data message 22
4.3.4 Control Message (SND_UD) 23
4.3.5 Control Message (SND_UD2) 25
4.3.6 Clock synchronisation message 27
4.3.7 On-demand data message 30
4.3.8 Unencrypted message 32

4.3.9 Installation message 32

5 Encryption Layer 34
5.1 Mode 9 Configuration Word Structure 34
5.2 Encrypted Message Structure 35
5.3 Initialisation Vector 35
5.4 Invocation Counter 36

6 Application Layer 37
6.1 Meter Value Transfer 38
6.2 Commands 38
6.2.1 Set Date and Time Procedure 38
6.2.2 Clearing the Status Word 39
6.2.3 Set new key 39
6.3 Readout List 40
6.3.1 Changing the readout list 41
6.3.2 Terminating the FAC 41
6.3.3 Reading the Status word 42
6.4 Variable Data Blocks 43
6.4.1 Equipment Identifier 43
6.4.2 Remote read of firmware and hardware versions 43
6.4.2.1 Detailed version info 44
6.4.3 Time stamp 45
6.4.4 Gas Meter specific data blocks 45
6.4.4.1 For hourly messages: 45
6.4.4.2 Gas Meter specific data blocks for 5-minutes messages: 47
6.4.5 Thermal (heat / cold) Meter specific data blocks for 5 min. and hourly values 48
6.4.6 Water Meter specific data blocks for 5 min. and hourly messages 49
6.4.7 Slave E-Meter specific data blocks for 5 min. and hourly messages 49
6.5 Key Management Procedures 49
6.5.1 Key Exchange Procedures 50
6.5.2 Key Management Requirements and encryption requirements 54
6.5.3 Security mode 9 and AES-GCM as its encryption mechanism 55

7 FIRMWARE UPDATE 57
7.1 End to end overview 57
7.2 Manufacturer to M-Bus device view 58
7.2.1 Manufacturer to CS view 59
7.2.2 CS to M-Bus device view 60
7.2.3 CS to E-Meter view 61
7.2.4 E-Meter to M-Bus device view 62

7.3 Firmware upgrade image structure....63
7.3.1 Header Section....63
7.3.2 Firmware upgrade states....65
7.3.3 General structure of used VIB codes....65
7.3.4 Firmware upgrade messages....66
7.3.5 Firmware upgrade status report response....66
7.3.6 The firmware update request block status....67
7.3.7 Firmware upgrade start....67
7.3.8 Firmware upgrade send data....69
7.3.9 Firmware upgrade validate....69
7.3.10 Firmware upgrade activate....69
7.3.11 Firmware upgrade cancel....70
7.3.12 Firmware upgrade request status report....70
7.3.13 Firmware upgrade request block status....70
7.3.14 Reboot of the E-meter....71
8 Power supply....71
8.1 Power outage....71
9 Installation procedures....72
9.1 General installation procedures....72
9.2 M-Bus Device State....72
9.3 Wireless device address....72
9.4 M-Bus Device Binding....73
9.5 E-Meter interaction....73
9.6 Local M-Bus Binding Procedure....74
10 Backwards CompatIbIlity....77
11 Interference between wireles M-bus and LTE....78
11.1 CSMA mechanism....79
11.2 Blocking filters....81
APPENDIX A: P2 – P3 mapping....82
APPENDIX B: Message examples....85
APPENDIX C: ESMR5 button process....98
APPENDIX D: Vendor specific error bits....99
APPENDIX E: Firmware update flow charts....100

1INTRODUCTION

1.1Scope

This document provides a companion standard for an Automatic Meter Reading (AMR) system for electricity, thermal, (heat & cold), gas, water and hot water meters. The scope of this standard is on:

- Residential electricity meters
- Residential thermal (heat & cold) meters
- Residential gas meters
- Residential water meters

This companion standard focuses on the P2 interface for Gas, Thermal (heat / cold) and Water meters.

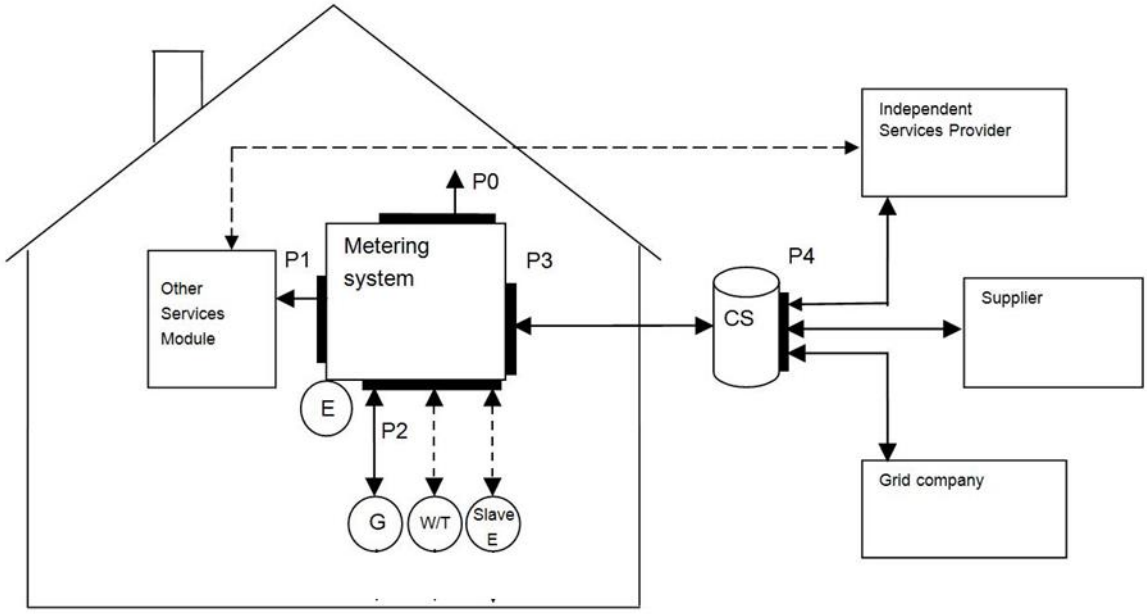


Figure1: Meter interfaces overview.

The goal of this companion standard is to reach an open, standardized protocol implementation and functional hardware requirements related to the communication between several types of meter and an electricity meter. The features described as normative in the EN 13757 documents (ref section 1.3) need to be implemented unless specified otherwise in this document.

1.2System architecture

This companion standard focuses on the communication between E-meters that are connected to the Central System (CS) and the M-Bus devices that are connected to that meter (including Slave E-meter). This communication is based on the M-Bus References to the M-Bus standard that are included in section 1.3. This companion standard only includes deviations, clarifications or additions to the standard as defined in the relevant standard documents.

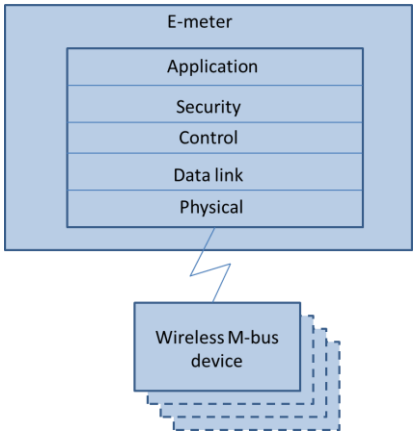


Figure 2: System architecture

Only wireless communication is supported.
Wireless communication is described in EN 13757-4. For wireless communication the electricity meter functions as Other device according to M-Bus terminology while the wireless M-Bus device initiates communication and functions as Meter.

The electricity meter will gather and store information from all connected M-Bus devices and makes this information available to the CS.

The maximum number of M-Bus devices associated with a single E-Meter is four. The data requirements of the CS are based on NTA 8130 (ref. section 1.3).

The payload of communication messages between Electricity meter and M-Bus devices must be encrypted and authenticated (Security Mode 9) whenever the standard supports this. By exception: Until the first User key is send to the G-meter, there is a short period of time where some messages (5 minute values and hourly values) are not encrypted. For commands the following is applicable:

- A time-set before the User key is set, must be sent with Security Mode 0 (no encryption). Once the User key is set, this command must be sent with Security Mode 9.
- A key change must always be sent with Security Mode 0 (no encryption).

- The confirmation of the installation request must always be sent in Security Mode 0 (no encryption). The Send_IR message is send with Security Mode 0 before the User key is set.

1.3Normative references

The following standards are referred to in this company standard. For undated references the latest edition applies.

EN 13757-2:2004	Communication systems for and remote reading of meters – Part 2: Physical and link layer
EN 13757-3 Draft version April 2015 N496	Communication systems for and remote reading of meters – Part 3: Dedicated application layer
EN 13757-4:2013	Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)
NTA 8130 NL:2007	Netherlands Technical Agreement -“Minimum set of functions for metering of electricity, gas and thermal energy for domestic customers”
DLMS Blue book 12th edition	COSEM Identification System and Interface Classes
FIPS-197	ADVANCED ENCRYPTION STANDARD (AES), published by the National Institute of Standards and Technology (NIST), USA.
AmvB	Algemene maatregel van Bestuur “Besluit op afstand uitleesbare meetinrichtingen”

Table 1: Normative References

Functional requirements for the metering system are defined in the NTA Requirements document (NTA 8130:2007).

1.4Document structure

The information in this document is structured according to the various communication layers as depicted below.

	Wireless
Application: Data structures, data types, actions	EN 13757-3
Encryption	EN 13757-3
Control: message flow	EN 13757-4
Data Link: transmission parameters, addressing, data integrity	EN 13757-4
Physical: cable, bit representation, bus extensions, topology, electrical specifications.	EN 13757-4

Table 2: document structure

Starting with the application level, each level defines layer specific header and trailer fields that must be added to the message before it can be send.

Note that the order of the detailed description of each layer is bottom up, so the Physical layer is described first. In the appendix B various message examples are given.

1.5Document list

Following table shows the complete set of documents that build up the Enexis Smart Meter Requirements, of which this document is a part of.

#	Document name postfix	description
[1]	Main	The main document of the Smart Meter Requirements, containing all definitions and most of the use cases and requirements
[2]	P1	Companion standard P1
[3]	P2	Companion standard P2
[4]	P3	Companion standard P3
[5]	LTE	Additional document describing the requirements for the LTE infrastructure as part of the Smart Meter Specification.
[6]	Uniform binding process	Uniform binding description
[8]	EnexisM-Bus RF performance_IMST_Final_1.0	Requirements for wireless M-Bus devices
[9]	Enexis_WirelessMBusCommunicationAndLTE_1v2.pdf	Theoretical analysis of the interference
[10]	Enexis_Interferential_Scenario Simulations_1v2.pdf	Results of simulations of the LTE and wM-Bus interference
[11]	Interference LTE on wM-Bus v1.1.pdf	Summary and conclusions of [9] and [10]

Table 3: Document List

2PHYSICAL LAYER

The physical layer of the P2 port is only wireless and is described below.

2.1Wireless connection

The wireless P2 port uses the M-Bus physical layer of EN 13757-4 (RF = radio frequency). The communication except the 5 minutes data messages shall be established according to the bidirectional sub-mode T2. In this mode of operation, the M-Bus device regularly transmits the readout value. Once per 24h it is able to receive a response from the E-meter for a very short period. Then the M-Bus device turns into sleep mode until its next transmission. The T2 parameters are defined in EN 13757-4 and are all mandatory. Since the wireless M-Bus device will be deployed in very difficult situations, the highest performance class is demanded. The transmit power shall be according to performance class H_T (+5 dBm transmitter for the M-Bus device, +8dBm transmitter for the E-meter). The receiver sensitivity and blocking performance shall be according to performance class H_R (min. sensitivity of -100dBm). The measurement of the radio performance will be as specified in EN 13757-4 section 4.3. Modulation is FSK in TX mode in accordance with the EN 13757-4 for T1, T2 and C1 messages. The 5 minutes data messages will use C1-mode with full frame messages.

When the M-Bus device is the transmitter, the header of the preamble sequence shall contain n≥19 01-patterns before the synchronisation word (0000111101), as specified in the EN 13757-4 standard.
However, the E-meter shall already meet the receiver performance requirements with a maximum of 19 01-patterns.
The E-meter may support the “capture effect” and detect other (new or stronger) transmissions based on the part of the preamble header while receiving another frame.

When the E-meter is the transmitter, the header of the preamble sequence shall contain n≥15 01-patterns before the synchronisation word (0001110110), as specified in the EN 13757-4 standard.
However, the M-Bus device shall already meet the receiver performance requirements with a maximum of 15 01-patterns.

Performance requirements of the antenna (sensitivity, ERP) can be found in the M-Bus RF performance document [8].

3DATA LINK LAYER

The Link transmission procedures of EN 60870-5-2 are used. The following section describes the specific usage of the link layer.

3.1Wireless Connections

For the wireless M-Bus link layer the format class FT3 of EN 60870-5-1 and a telegram structure for a frame with variable length according to EN 60870-5-2 shall be used. Note that the Start bytes 05h 64h are replaced by the Preamble Chip Sequence as described in EN 13757-4. This frame format includes a length field (L), a control field (C) and an address field (A). The general format A of EN 13757-4 shall be used for the protocol header, see Table 4, with deviations as discussed in the following.

Field	Remark
PL	Preamble
L	Length
C	Control field
M	Manufacturer ID
A	Address field of the sending Meter
Checksum	Specified in EN 60870-5-1
Link user data	Variable length data block
Checksum	Specified in EN 60870-5-1
…	…
Link user data	Variable length data block
Checksum	Specified in EN 60870-5-1
‘01’b or ‘10’b	Postamble

Table 4: Frame format FT3 (general format A).

3.1.1Length field (L)

The length field specifies the message length in bytes, excluding length and CRC fields. The maximum length of a single telegram is 255 bytes.

3.1.2Control field (C)

The control field specifies the frame type. In deviation from EN 13757-4, the allowed telegram types are: SND_NKE, REQ_UD2, RSP_UD, SND_UD, SND_UD2, SND_NR, ACK, SND_IR and CNF_IR. Not allowed are REQ_UD1, ACC_NR and ACC_DMD.

The frame count bit (FCB) of the C-Field is ignored. At the Control Layer, the Access Number shall be used to detect communication failures.

3.1.3Manufacturer Identification field (MAN)

An 2 byte field is used to identify the manufacturer as specified in clause 5.6 of EN 13757-3.

3.1.4 Address field (A: ID | VER | DEV)

An 6 bytes address field is used to identify the sender (source) as defined in EN 13757-4 Annex E. The A-field shall be generated as a concatenation of Identification Number (ID-field: 4 octets), Version identification (VER-field: 1 octet) and Device Type identification (DEV-field, 1 octet), all specified in EN 13757-3. See also Note 1.

If the M-Bus device is the sender, the address at the Data Link Layer and the address at the Control Layer will be the same Meter address (LLA and ALA respectively in EN 13757-4 Annex E).
Also the E-meter will have a valid Data Link Layer address.[1,]

3.1.5 Timing

EN 13757-4 details about various timing aspects at Data Link Layer level which will be further specified in this section.

3.1.5.1 Installation Mode

The M-Bus device will be delivered by the vendor from the factory in installation mode. In that mode the M-Bus device will transmit a SND_IR every hour as long as the M-Bus device does not receive an appropriate response (CNF_IR) from the designated E-meter.
If the installation mode is activated or re-activated by the button press, the M-Bus device shall transmit SND_IR messages every minute during 30 minutes as long as the M-Bus device does not receive an appropriate response (CNF_IR) from the designated E-meter. After 30 minutes, it continues transmitting installation messages (SND_IR) once every hour until reception of an appropriate response (CNF_IR) from the designated E-meter. The installation mode can be activated or re-activated by the button press 3 times per day (if the battery protection credits are sufficient at that time).
Once the M-Bus device receives a CNF_IR message from the designated E-meter, the M-Bus device will set the binding flag in the status word. As soon as the binding flag is set this will also be a trigger for the device to allow a Frequent Access Cycle for every T-mode communication (every hour). This FAC availability will stop as soon as the M-Bus device has successfully received a new user-key and encryption mode 9 is active. From this point on the M-Bus device will go back into one FAC per 24 hours. A re-binding to the same E-meter will not set the binding flag again and will not trigger the device to allow a FAC every hour again.

[1] EN 13757-4 allows for different addressing of the meter and the RF module (radio). In this document it is assumed that the radio is integrated with the equipment (E-meter and M-Bus device) and only a single address (short ID of the meter) is defined.

3.1.5.2 Regular hourly user data message

The transmission of the regular hourly user data messages (SND_NR with billing data) from the M-Bus device shall have a randomized timing with true randomization. Care must be taken so that the random transmission interval fits between 1 minute to 10 minutes window after the whole hour that is allowed for M-Bus transmissions (requirement M4.5.7 in the ESMR Main document), for instance by applying an appropriate offset. The hourly transmission shall always transmit the new hourly meter reading and never starts before the meter data that needs to be transmitted is available. Besides the new hourly value also the 3 previously recorded hourly values will be transmitted in the same message.
The Control Layer shall support the required Access Number initialisation and increments.
The CC field in the Extended Link Layer of the M-Bus device shall determine whether bidirectional communication is possible or not.

All messages from G-meter (“Meter”) tot E-meter (“Other”) in T-mode use the Extended Link Layer (for signalling the availability of the FAC). 5 minute messages are in C-mode and do not use the ELL. Also messages from “Other” to “Meter” (E-meter to G-meter) don’t use the ELL.

Every hourly message from the M-Bus device will allow the Frequent Access Cycle to be opened, but the M-Bus device will limit the amount of FAC’s to once per 24 hours. When battery credits of the M-Bus device do not allow any further Frequent Access Cycle possibilities the M-Bus device will no longer listen to E-meter messages after transmitting of T-mode messages.
Once per 24 hours, at 00:00h, the hourly user data message contains additional (important) static data, like status word and equipment identifier, see section 6.3.

3.1.5.3 Regular 5 minutes user data message

Every 5 minutes the M-Bus device will send regular 5-min messages as described in chapter 4.3.3. The M-Bus device shall have a randomized timing for the 5 minute messages with true randomization within a 10 second window after the 5 minutes boundary

4CONTROL LAYER

The Control Layer is inserted here to specify and clarify how the message flows are managed. This layer is not a formal part of the M-Bus series (EN 13757), but it combines the control field (C-field) of the Data Link Layer, the control information field (CI-field) of the Transport Layer and related elements to control exchange of messages between the E-meter and the M-Bus device.

4.1Allowed control elements

The following table defines the messages and their response that shall be used for the message transactions. [Table 5] contains the C-field and CI-field control elements for wireless connections. For security reasons, all combinations of C and CI codes that are not described in this section shall be rejected (meaning: no further processing of the message).

WIRELESS M-Bus connection				
Purpose	Initiator	Direction data	Message	Response
Normalisation message: reset link, stop FAC	E-meter	<none>	SND_NKE C=40h; CI=80h	<none>
Meter data message: billing data, status, version	M-Bus device	M-Bus device to E-meter	SND_NR C=44h; CI=7Ah	<none>
On-demand data message: billing data, status	E-meter	M-Bus device to E-meter	REQ_UD2 C=5Bh; CI=80h	RSP_UD C=08h; CI=7Ah
Control message: readout list	E-meter	E-meter to M-Bus device	SND_UD2 C=43h; CI=5Bh	RSP_UD C=08h; CI=7Ah
Control message: clock synchronisation	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=6Ch	ACK C=00h; CI=8Ah
Unencrypted message: set key (conf. word = 00h)	E-meter	E-meter to M-Bus device	SND_UD2 C=43h; CI=5Bh	RSP_UD C=08h; CI=7Ah
Installation message: broadcast and registration	M-Bus device	<none>	SND_IR C=46h; CI=7Ah can be sent encrypted (once the key is set) or unencrypted (before the key is set) because all information is available in the header	CNF_IR C=06h; CI=80h (conf. word = 00h)
Control message: immediate readout	E-meter	E-meter to M-Bus device	SND_UD2 C=43h; CI=5Bh	RSP_UD C=08h; CI=7Ah

Table 5: Control Layer for wireless connections with allowed C-field and CI-field combinations

Message Type	Message from E-meter	Response M-Bus device	Trigger for message
SND_NKE	Normalization message	End FAC, return readout list to normal	No scheduled messages
SND_UD*	- Clock synchronization*	Ack	- Internally or CS
SND_UD2	- Set key (FUAK) - Set key (user key) - Reset status word - Change readout list (Detailed version info**) - Change readout list (FW update)	- RSP_UD (daily (long) hourly message) - RSP_UD (daily (long) hourly message) - RSP_UD (daily (long) hourly message) - RSP_UD with Version info - RSP_UD (mostly FW upgrade status report)	- CS - CS - after event G-meter - Internally or CS - CS
CNF_IR	Confirmation installation request	RSP_UD (daily (long) hourly message)	SND_IR

* Clock synchronization is the only message which is send with a SND_UD, the rest of the messages are send with SND_UD2.

** The Detailed version info is mandatory to ask for all versions (VIF/VIFE = FDh 0Ch; FDh 0Dh; FDh 0Eh; FDh 0Fh).

Table 5a: Response from M-Bus device on messages from E-meter

SND_NKE:

SND_NKE is a message to terminate the FAC if no further messages are in queue. This will also reset the readout list to the daily (long) hourly message.

Clock synchronization:

The clock of a G-meter shall not deviate more than 60 seconds from the E-meter. To ensure this the E-meter can synchronize the clock of the M-Bus device. The clock synchronization message is send with a SND_UD, the response is an Ack.
An E-meter will only send a clock sync with a SND_UD. All other commands have to be sent with a SND_UD2.
Trigger: See Use Case 13 in Main document.

Set Key (FUAK):

It is possible to change the Firmware Update authentication Key. When this key is changed, the E-meter will not change the encryption status (this is for the user key). The G-meter will trigger an event (part of clarification P3.3) when the FUAK is not accepted. The FUAK is send with a SND_UD2, the G-meter will respond with a RSP_UD (daily (long) hourly message). Only the most recent received key must be sent to the G-meter.
Trigger: Set key (FUAK) is triggered by the CS.

Set Key (User key):
When a E-meter sends a SND_UD2 to change the user key, internally the encryption status is set to 3 (this will only be triggered by sending the message over P2 port and not when queuing the message for the next FAC). When the G-meter accepts the user Key, it will respond with an RSP_UD (daily (long) hourly message) encrypted and authenticated with the new key. This will internally trigger in the E-meter the encryption status to 4 (see P3.17). Only the most recent received key must be sent to the G-meter.
Tigger: Set Key (user key) is triggered by the CS.

Reset status word:
When a G-meter reports an event, the E-meter will register this event in the M-Bus event log (see clarification session P3.7). In addition the E-meter queue's a reset status word message (SND_UD2), where the status word is reset (with a mask). The G-meter responds with a daily (long) hourly message. If the error on the G-meter still exist, the G-meter will report this in the daily (long) hourly message (status word). The status word will be reset only once during a FAC.
Trigger: The message Reset status word is triggered internally by the E-meter, when a message is send by the G-meter where a bit in the status word is set.

Detailed version info:
With the request for detailed version info, it is possible to extract HW and SW versions of the G-meter. There are 4 VIFE's to get all the info. It is mandatory to ask all the VIFE's in one request, so the FAC messages are used as effective as possible. The G-meter will respond with an RSP_UD with the detailed version info which has been requested. The detailed version info is requested with a SND_UD2.
Trigger: the detailed version info is requested by the E-meter after the first set user key and after every successful and unsuccessful FW update of the G-meter.

FW Update:
The FW update is started with a SND_UD2 Change Readout List: FW upgrade request status. After this message the G-meter will open the extended FAC and the update process can started. The more detailed information about the FW update of the G-meter, can be found in chapter 7 of the P2 companion standard.

Priority of messages:

It is necessary to prioritize the possible messages from E- to G-meter. If a message cannot be send in a FAC for some reason, the message is postponed to the next FAC.

In a FAC the following priorities are set:
1. Reset status word MUST be performed if the E-meter has noticed a G-meter event.
2. Key changes will also be queued for the First FAC after receiving the key change message from the CS. The user key is always sent first and must be in use before the FUAK key is sent. This must be covered by the CS. The E meter will not check this.
3. Time synchronization is queued whenever the G-meter is sending 5 minutes values outside the specified window.
4. Change readout list: Read detailed version information
5. Change readout list: FW update will always be started at the First FAC after receiving the FW update for the G-meter, however the FW update start message will be performed as latest possible message in that FAC.

A Change readout list must be done at the end within a FAC, because the RSP_UD will be according the last readout list.

4.2Common control elements

4.2.1Data Headers

Depending on the CI code, the message shall contain a short or a long header as is specified in EN 13757-3, see Figure 3. Specifically, CI codes 7Ah and 8Ah shall use a short data header and CI codes 5Bh and 80h shall use a long data header. The long data header address is in the format of the short equipment identifier.

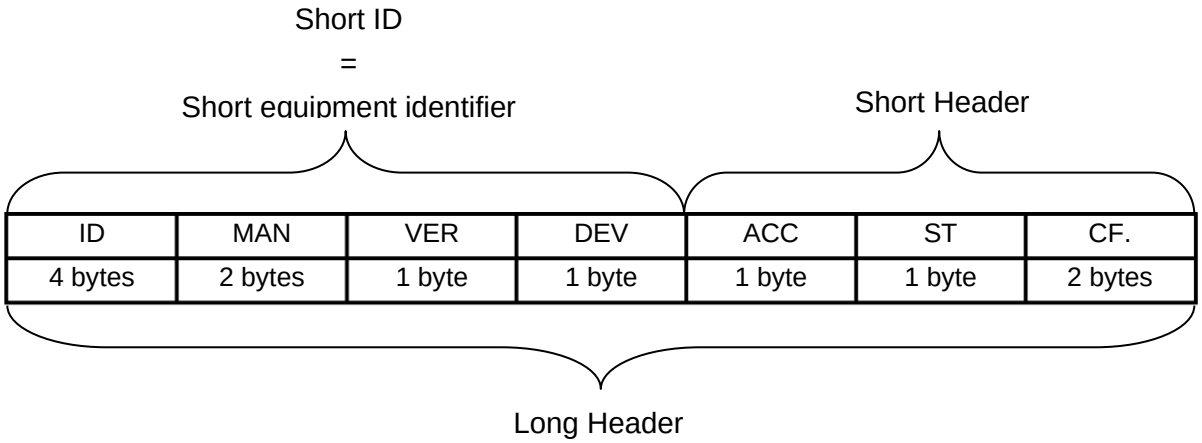


Figure 3: Definition of long header, short header and Short ID.

4.2.2Short Equipment Identifier (Short ID: ID | MAN | VER | DEV)

The M-Bus and the E-meter device shall use the concatenation of Identification Number (ID-field: 4 octets), Manufacturer identification (MAN-field: 2 octets), Version identification (VER-field: 1 octet) and Device Type identification (DEV-field, 1 octet), all specified in EN 13757-3, as short equipment identifier (Short ID), see Figure 3. The Short ID is added because the encrypted full equipment identification is hidden during certain installation processes. The uniqueness of the Short ID (in the Netherlands) shall be guaranteed by the manufacturer over the lifetime of the meter type. The Identification Number is derived from the 17 digits Equipment Identifier. The last 8 digits of the 10 digits serial number within the Equipment Identifier are used as Identification Number and packed in 4 bytes BCD format.

Notice that for wireless, the link layer address (see 3.1.4) is similar but not identical to the Short ID because the MAN and ID fields are swapped. Since the fields are stored in individual P3 objects of the E-meter, this should be no issue for the central system. In addition, if the E-meter sends a CNF_IR message, the M-Bus device registers the address of the E-meter in order to be able to show it on its display. For all other incoming messages the address of the E-meter shall be ignored.

4.2.3Version field

The version field in the fixed header is used to transfer the hardware version of the M-Bus device. This version will remain static for the specific device during its life time. A firmware update shall not change this version. The initial version of the M-Bus devices will be 50h (indicating a ESMR5.x device).The “5” is stored in the high nibble; the “0” is stored in the low nibble of the version field.

The reason for this is that if the version is updated (for instance by loading a new firmware version in the M-Bus device) then the radio address will change and the connection with the E-meter will get lost. Therefore the version needs to be static referencing the hardware version of the device.

4.2.4Access No. (ACC)

The access number in the data header (ACC-field) will be maintained by the M-Bus device as specified in EN 13757-3 section 5.9. As stated the Access Number of the M-Bus device shall be initialised by a random number which will be independent for each M-Bus device.
Note: the T- and the C1-messages have independent Access numbers.

4.2.5Status (ST)

The status byte in the header is not protected and vulnerable for compromising the communication. Therefore it is not used for status information as described in EN 13757-3 section 6.5.6 but it is used to transfer the RSSI value. The status of the M-Bus device itself can be retrieved using the DIF/VIF combination described in 6.3.3.
The RSSI value transmitted by the M-Bus device is the received signal strength that indicates the reception of the E-meter messages by the M-Bus device’s receiver.
The RSSI value transmitted by the E-meter is the received signal strength that indicates the reception of the M-Bus device messages by the E-meter’s receiver.
The RSSI will be transmitted as specified in EN 13757-3 section 6.5.7 ‘Status byte in partner messages’.

4.2.6Configuration word (CW)

The mode 9 configuration word is described in chapter 5.1.

4.3Wireless Connections

Wireless hourly messages between the E-meter and the M-Bus device shall be exchanged in T2-mode of the wireless M-Bus protocol according to the specification EN 13757-4. This means that for hourly meter data messages, the M-Bus device behaves as a primary station (described in EN 60870-5-2) and transmits periodically unacknowledged messages with billing data to the E-meter. The average period is T_{NOM} with randomized variation as discussed in section3.1.5. The message type is SND_NR (Send / No Reply) with a short address header. If the E-meter has a command, a request or data to send to the M-Bus device, it shall use the so-called Frequent Access Cycle (FAC) method (section 11.6.3.3 in EN 13757-4). It pro-

vides the E-meter a short access window (response delay t_{RO} specified in EN 13757-4) after a T1-transmission of the M-Bus device until the FAC reached the maximum number of transmissions.

For the FAC the following applies

- maximum 6 cycles = maximum 6 transmissions from M-Bus device during FAC
- FAC time out = max 6 transmissions, 30 seconds
- FAC transmission delay = transmission delay: N=5.
  Remark: During FW update it is allowed to extend the FAC and set N to 2.

The M-Bus device will allow to open a FAC every hour until the maximum allowance of one credit per 24 hours has been used.

The wireless message transactions timing diagram for hourly messages is summarized in Figure 4 and detailed in the subsequent sections. The figure shows two sides of the communication channel. One is the E-meter with the symbolic data link layer address (LLA) E-MTR and the other is the M-Bus device with the symbolic application layer address (ALA; actually Transport layer address) being equal to the data link layer address (LLA) M-DEV. The vectors in the message exchange timing diagram signify directional messages with the data link layer message type (with C-field and data link layer address), the control information of the application layer followed by the application layer address (if applicable) and the access number (ACC). The access number values are examples to show the behaviour. The EN 13757 specifications are ambiguous on the behaviour of the access number[2]. This document follows the EN 13757-4 specification and asynchronous transmissions (e.g. the FAC) starts with a newly initiated ACC that is incremented every subsequent asynchronous transmission of the M-Bus device.
The other content is fixed and depending only on the type of message and its origin. The data link layer address shall always be the address of the sender, but as stated in section 4.2.2 (address field for wireless): the data link layer address of the E-meter can be ignored except for the CNF_IR message.

The 5 minutes data messages use C1-mode. After a C1 message the M-Bus device will not listen to E-meter messages there will be no possibility for the E-meter to open a FAC after a 5 minutes data message.

[2] EN-13757-3 states “For every asynchronous transmission between two synchronous telegrams the meter shall use the access number from the last synchronous transmission.” - i.e. the access number is frozen during the frequent access cycle. Annex E of EN 13757-4 shows an incrementing ACC.

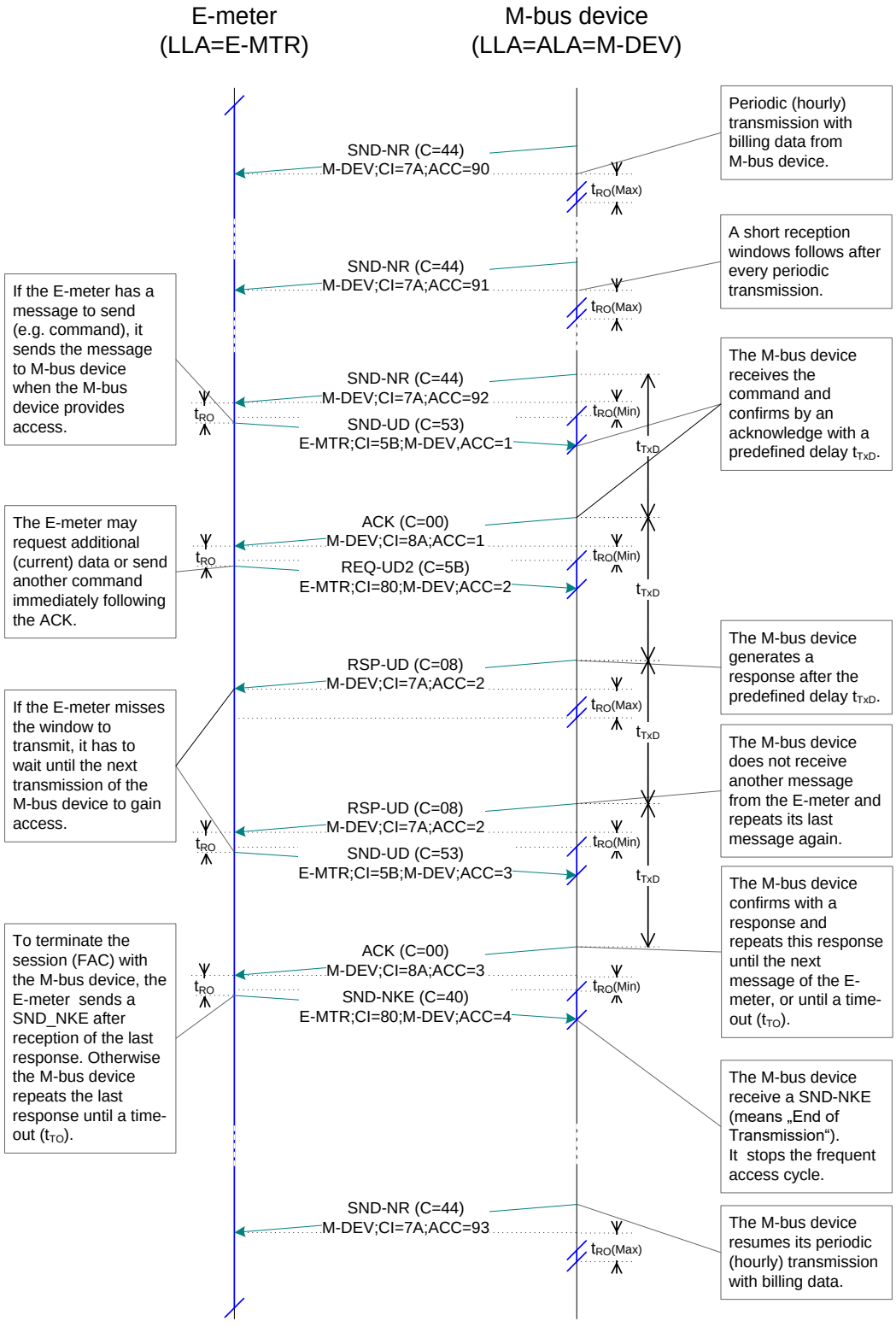


Figure 4: Timing diagram of wireless message transactions in T2-mode with short address.

4.3.1Normalisation message

The E-meter and G-meter resumes to normal operation mode (ends FAC for instance) by sending a short frame to the specific M-Bus device: SND_NKE**.** See table 6**.**

Field		Hex	Remark
Preamble of physical layer			
L-Field		L-0	Length xx Bytes
C-Field		40h	SND_NKE
M-Field of sender		M-0	Manufacturer identification of the E-meter
		M-1	
A-Field of sender		A-0	Address of the E-meter
		A-1	
		A-2	
		A-3	
		A-4	Version of the E-Meter
		A-5	Device Type of the E-Meter
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI-Field		80h	Transport layer (long) from Readout device to the Meter
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access No.		AC-0	Access Counter (of E-meter)
Status		ST-0	RSSI value
Configuration Word		01h	Security Mode 9, Tag present
		29h	
Len E		00h	Mode 9 header - number of encrypted bytes
Len U		00h	Mode 9 header - number of unencrypted bytes
CTR		CT-3	Mode 9 header – counter (MSB first)
		CT-2	
		CT-1	
		CT-0	
GCM authentication tag		AT-0	12 bytes tag
		..	
		AT-11	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Table 6: Normalisation message

There is no response from the M-Bus device; it just accepts this message and starts the periodic transmission of the meter data message as described in the following section.

4.3.2 Hourly meter data message

The M-Bus device transmits unsolicited meter data message without reply: SND_NR. See table 7.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	44h	SND_NR
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Address of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	8Ch	Extended Link Layer 1
CC-Field	24h	Synchronized, Accessible
ACC-Field	ACC-0	ELL Access Counter
CI-Field	7Ah	Transport layer with short header
Access No.	AC-0	Access Counter (of M-Bus device)
Status	ST-0	RSSI value
Configuration Word	01h	Security Mode 9, Tag present
	29h	
Len E	LE-0	Mode 9 header – number of encrypted bytes
Len U	00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR	CT-3	Mode 9 header – counter (MSB first)
	CT-2	
	CT-1	
	CT-0	
Encrypted Variable Length Data Blocks (Records) (ref section 6.4.4.1)		
GCM authentication tag	AT-0	12 bytes tag
	..	
	AT-11	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Table 7: Hourly meter data message

Remarks

- The short header is sufficient (and mandatory) since the target will always be the designated E-meter.
- This is a template frame, mainly to indicate the mandatory bits and pieces. There are no variable blocks inserted here; the length field depends on this content.
- Before the User key is set, at installation time, the message must be sent with Security Mode 0 (configuration word equal to 00h).

There are 2 types of hourly user data messages for gas meters, see Readout list specification section 6.3:

- The normal (short) hourly meter data message, to be sent on every hour except 00:00h.
- The daily (long) hourly meter data message, to be sent once per day on 00:00h.

It is good to be aware of the fact that a G-meter is running on UTC time only. This means that the E-meter can expect this messages at 01:00h or at 02:00h local time, depending on Daylight Saving Time in the Netherlands.

4.3.3 5-min user data message

The gas meter transmits the volume index and timestamp every 5 minutes. The transmission uses mode C1 with encryption (and authentication) according to Security Mode 9 and frame format B.
The transmission packet consists of 52 bytes plus preamble and sync word. The total packet consists of 60 bytes (480 bits). See table 8.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	44h	Send no reply
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Address of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
CI-Field	7Ah	Transport layer with short header
Access No.	AC-0	
Status	ST-0	RSSI value

Configuration word	01h	Security Mode 9, Tag present
	29h	
Len E	LE-0	Mode 9 header – number of encrypted bytes
Len U	00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
Counter	CT-3	Mode 9 header – counter (MSB first)
	CT-2	
	CT-1	
	CT-0	
Encrypted Data Block as described in section 6.4.4.2		
GCM authentication tag	AT-0	12 bytes tag
	..	
	AT-11	
Checksum	CS-0	2 bytes checksum of frame format B telegram
	CS-1	
Postamble of physical layer		

Table 8: 5 minute user data message

4.3.4Control Message (SND_UD)

The E-meter sends control and configuration information to the specific M-Bus device within the so-called frequent access cycle (FAC). It is started with a valid transmission from the E-meter just after a regular meter data transmission from the M-Bus device, which will then be in receive mode during a short window (t_{RO}). The valid transmission may just well be control and configuration information, sent with message type SND_UD using CI=5Bh and long header. Unencrypted messages are described in table 9.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	53h	SND_UD
M-Field	M-0	Manufacturer identification of the E-meter
of sender	M-1	
A-Field	A-0	Address of the E-meter
of sender	A-1	
	A-2	
	A-3	
	A-4	Version of the E-Meter
	A-5	Device Type of the E-Meter
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI-Field	5Bh	Application data from E-meter to M-Bus device with long header

Field		Hex	Remark
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access No.		AC-0	Access Counter (of E-meter)
Status		ST-0	RSSI value
Configuration Word		01h	Security Mode 9, Tag present
		29h	
Len E		LE-0	Mode 9 header – number of encrypted bytes
Len U		00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR		CT-3	Mode 9 header – counter (MSB first)
		CT-2	
		CT-1	
		CT-0	
Encrypted Variable Data Blocks (Records) (ref section 6.4)			
GCM authentication tag		AT-0	12 bytes tag
		..	
		AT-11	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Table 9: Control message SND_UD

The response of an M-Bus device is an acknowledgement: ACK. See table 10.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	00h	ACK
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Address of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	

Field	Hex	Remark
CI	8Ch	Extended Link Layer 1
CC-Field	80h	limited access
ACC-Field	ACC-0	ELL Access Counter
CI-Field	8Ah	Transport layer with short header
Access No.	AC-0	Access Counter (copied from SND_UD)
Status	ST-0	RSSI value
Configuration Word	01h	Security Mode 9, Tag present
	29h	
Len E	00h	Mode 9 header – number of encrypted bytes
Len U	00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR	CT-3	Mode 9 header – counter (MSB first)
	CT-2	
	CT-1	
	CT-0	
GCM authentication tag	AT-0	12 bytes tag
	..	
	AT-11	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Table 10: Response of M-Bus device on SND_UD

4.3.5Control Message (SND_UD2)

The E-meter sends control and configuration information and requires data in the immediate reply. This is sent with message type SND_UD2 using CI=5Bh and long header, the reply is a RSP_UD message. See table 11.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	43h	SND_UD2
M-Field of sender	M-0	Manufacturer identification of the E-meter
	M-1	
A-Field of sender	A-0	Address of the E-meter
	A-1	
	A-2	
	A-3	
	A-4	Version of the E-Meter
	A-5	Device Type of the E-Meter
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI-Field	5Bh	Application data from E-meter to M-Bus device with long header

Field		Hex	Remark
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access No.		AC-0	Access Counter (of E-meter)
Status		ST-0	RSSI value
Configuration Word		01h	Security Mode 9, Tag present
		29h	
Len E		LE-0	Mode 9 header – number of encrypted bytes
Len U		00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR		CT-3	Mode 9 header – counter (MSB first)
		CT-2	
		CT-1	
		CT-0	
Encrypted Variable Data (Records) (ref section 6.4)			
GCM authentication tag		AT-0	12 bytes tag
		..	
		AT-11	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Table 11: Control message SND_UD2

The M-Bus device responses with (encrypted) meter data: RSP_UD. See table 12.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	08h	RSP_UD
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Address of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	

Field	Hex	Remark
CI	8Ch	Extended Link Layer 1
CC-Field	80h	limited access
ACC-Field	ACC-0	ELL Access Counter
CI-Field	7Ah	Transport layer with short header
Access No.	AC-0	Access Counter (of M-Bus device)
Status	ST-0	RSSI value
Configuration Word	01h	Security Mode 9, Tag present
	29h	
Len E	LE-0	Mode 9 header – number of encrypted bytes
Len U	00h	Mode 9 header – number of unencrypted bytes always zero for mode 9)
CTR	CT-3	Mode 9 header – counter (MSB first)
	CT-2	
	CT-1	
	CT-0	
Encrypted Variable Data (Records) (ref section 6.4)		
GCM authentication tag	AT-0	12 bytes tag
	..	
	AT-11	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Table 12: RSP_UD

4.3.6Clock synchronisation message

The E-meter sends the clock synchronisation control information with a specific SND_UD. If the User key is not set, this command must be sent unencrypted (Security Mode 0). When the User key is set, this command must be send encrypted and unencrypted clock messages shall be ignored from that point in time. See table 13 for an example of the encrypted command.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	53h	SND_UD
M-Field	M-0	Manufacturer identification of the E-meter
of sender	M-1	
A-Field	A-0	Short ID of the E-meter
of sender	A-1	
	A-2	

Field		Hex	Remark
		A-3	
		A-4	Version of the E-Meter
		A-5	Device Type of the E-Meter
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI-Field		6Ch	Time Sync to device
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access No.		AC-0	Access Counter (of E-meter)
Status		ST-0	RSSI value
Configuration Word		01h	Security Mode 9, Tag present
		29h	
Len E		LE-0	Mode 9 header – number of encrypted bytes
Len U		00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR		CT-3	Mode 9 header – counter (MSB first)
		CT-2	
		CT-1	
		CT-0	
Time Sync to device, encrypted (ref section 6.2.1)			
GCM authentication tag		AT-0	12 bytes tag
		..	
		AT-11	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Table 13: Encrypted clock synchronisation message

The response of an M-Bus device is an acknowledgement: ACK. See table 14.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	00h	ACK
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Short ID of the M-Bus device (=sender)
	A-1	

Field	Hex	Remark
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	8Ch	Extended Link Layer 1
CC-Field	80h	limited access
ACC-Field	ACC-0	ELL Access Counter
CI-Field	8Ah	Transport layer with short header
Access No.	AC-0	Access Counter (copied from SND_UD)
Status	ST-0	RSSI value
Configuration Word	01h	Security Mode 9, Tag present
	29h	
Len E	00h	Mode 9 header – number of encrypted bytes
Len U	00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR	CT-3	Mode 9 header – counter (MSB first)
	CT-2	
	CT-1	
	CT-0	
GCM authentication tag	AT-0	12 bytes tag
	..	
	AT-11	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Table 14: Response on an encrypted clock synchronisation message

4.3.7On-demand data message

The E-meter may request meter data on demand from the specific M-Bus device within the FAC using REQ_UD2 or SND_UD2. See table 15.

Field		Hex	Remark
Preamble of physical layer			
L-Field		L-0	Length xx Bytes
C-Field		5Bh	REQ_UD2
M-Field of sender		M-0	Manufacturer identification of the E-meter
		M-1	
A-Field of sender		A-0	Short ID of the E-meter
		A-1	
		A-2	
		A-3	
		A-4	Version of the E-Meter
		A-5	Device Type of the E-Meter
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI-Field		80h	Transport layer (long) without application data
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access No.		AC-0	Access Counter (of E-meter)
Status		ST-0	RSSI value
Configuration Word		01h	Security Mode 9, Tag present
		29h	
Len E		00h	Mode 9 header – number of encrypted bytes
Len U		00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR		CT-3	Mode 9 header – counter (MSB first)
		CT-2	
		CT-1	
		CT-0	
GCM authentication tag		AT-0	12 bytes tag
		..	
		AT-11	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Table 15: On demand data message REQ_UD2

The M-Bus device responses with (encrypted) meter data: RSP_UD. See table 16.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	08h	RSP_UD
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	A-field of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	8Ch	Extended Link Layer 1
CC-Field	80h	limited access
ACC-Field	ACC-0	ELL Access Counter
CI-Field	7Ah	Transport layer with short header
Access No.	AC-0	Access Counter (of M-Bus device)
Status	ST-0	RSSI value
Configuration Word	01h	Security Mode 9, Tag present
	29h	
Len E	LE-0	Mode 9 header – number of encrypted bytes
Len U	00h	Mode 9 header – number of unencrypted bytes (always zero for mode 9)
CTR	CT-3	Mode 9 header – counter (MSB first)
	CT-2	
	CT-1	
	CT-0	
Encrypted Variable Data Blocks (Records) (ref section 6.4)		
GCM authentication tag	AT-0	12 bytes tag
	..	
	AT-11	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Table 16: RSP_UD

Remarks

- This message may be helpful validating the performed action after a command.

4.3.8Unencrypted message

Specific control information, only in case of key exchangeand CNF_IR, must always be transmitted with an unencrypted message type. The E-meter sends this control and configuration information to the specific M-Bus device with the same SND_UD2 message as for the encrypted control message (see 4.3.4) and with the configuration word all zero (CW=00h) and Security Mode 0 will be used.

A time set must be transmitted with an unencrypted message type when the User key is not set. Once the User key is set, a time set must be transmitted encrypted.

4.3.9Installation message

The M-Bus device that is put in installation mode (manually or by other means) will transmit periodically installation requests: SND_IR (depending on whether the User key is set or not in Security Mode 9 or Mode 0). This message shall contain the Short ID. See table 17.

Field	Hex	Remark
Preamble of physical layer		
L-Field	L-0	Length xx Bytes
C-Field	46h	SND_IR
M-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Short ID of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	Version of the M-Bus device
	A-5	Device Type of the M-Bus device
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	8Ch	Extended Link Layer 1
CC-Field	80h	limited access
ACC-Field	ACC-0	ELL Access Counter
CI-Field	7Ah	Transport layer with short header
Access No.	AC-0	Access Counter (of M-Bus device)
Status	ST-0	RSSI value
Configuration Word	00h	Security Mode 0, message is encrypted & not authenticated.
	00h	
Variable Data Blocks (Records) (ref section 6.4) optional		
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Table 17: Unencrypted installation message of an M-Bus device

The E-meter confirms the installation using CNF_IR. See table 18.

Field		Hex	Remark
Preamble of physical layer			
L-Field		L-0	Length xx Bytes
C-Field		06h	CNF_IR
M-Field of sender		M-0	Manufacturer identification of the E-meter (or 00 00h) (this will be ignored by the M-Bus device)
		M-1	
A-Field of sender		A-0	Short ID of the E-meter
		A-1	
		A-2	
		A-3	
		A-4	Version of the E-Meter
		A-5	Device Type of the E-Meter
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI-Field		80h	Transport layer without application data
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access No.		AC-0	Access Counter (copied from of M-Bus device)
Status		ST-0	RSSI value
Configuration Word		00h	Security Mode 0, message is not encrypted & not authenticated.
		00h	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Table 18: Installation confirmation message

5ENCRYPTION LAYER

For all application level data during normal operation, encryption and authentication using Security Mode 9 as specified in EN 13757-3 is mandatory. The encryption algorithm used is AES-128 GCM (Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES)). Only Mode 9 and in specific cases Mode 0 (key change, timeset before User key is set and confirm installation request), shall be used.

5.1Mode 9 Configuration Word Structure

The Configuration word used in the control layer and in the encryption layer. The configuration word is coded as in table 19:

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved	Reserved	Authentication Tag size	Mode bit 4	Mode bit 3	Mode bit 2	Mode bit 1	Mode bit 0	Len U	Len E	KDF-selection 1	KDF-selection 0	Key-ID 3	Key-ID 2	Key-ID 1	Key-ID 0
R	T	O	M	M	M	M	M	U	E	D	D	K	K	K	K
0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	1

The word is configured as follows :

Field	Usage	Value
Key-ID	User key 1	1
KDF	Static key	0
LEN E	1 byte length	0
LEN U	1 byte length	0
Mode	Mode 9	9
Authentication Tag size	Tag present	1
Reserved	Reserved	0

Table 19: Mode 9 Configuration Word Structure

This gives a fixed value configuration word of 2901h after deployment. When there is no User key available, messages are sent with Security Mode 0. If a User key is available, messages are sent with Security Mode 9.

5.2Encrypted Message Structure

The structure of the encrypted M-Bus message is as shown in table 20:

Field	CI	HDR-1	HDR-CFG	Len E	Len U	CTR	E-Data	Tag
Size	1	X	2	1	1	4	N	12
Value	-	-	2901h	N	0	-	-	-

Table 20: Encrypted Message Structure

The size of the first part of the header depends on whether short or long header is used. The length of the un-encrypted section is always 0.

Control messages from the E-meter are always sent encrypted. The M-Bus device ignores unencrypted control messages (excluding key change command, time set command when the User key is not set, and installation confirmation messages).

The structure of the unencrypted M-Bus message is as shown in table 21:

Field	CI	HDR-1	HDR-CFG	Data
Size	1	X	2	N
Value	-	-	0000h	-

Table 21: Unencrypted Message Structure

5.3Initialisation Vector

A 12 byte IV is used as specified in EN 13757-3. This is constructed as in table 22:

MS Byte	11	10	9	8	7	6	5	4	3	2	LS Byte
ID (LSB)	..	..	ID (MSB)	MFT (LSB)	MFT (MSB)	Version	Dev. type	CNT MSB	..	..	CNT LSB

Table 22: Initialisation Vector

Where:

- ID is the Identification number of the M-Bus device
- MFT is the Manufacturer ID
- Version is as per M-Bus header Version
- Dev. type is the device type as per M-Bus header (e.g. 03 for gas)
- CNT is the Invocation Counter, specified in section 5.4

Note: The byte order of the GCM IV's will be considered as:
iv[1] = counter (LSB)
iv[2] = counter >> 8
iv[3] = counter >> 16
iv[4] = counter >> 24 (MSB)
iv[5] = device type
iv[6] = version
iv[7] = manufacturer >>8 (MSB)
iv[8] = manufacturer (LSB)
iv[9] = id >> 24 (MSB)
iv[10] = id >> 16
iv[11] = id >> 8
iv[12] = id (LSB)

5.4Invocation Counter

The Invocation Counter (referred to as the counter hereafter) used by Security Mode 9 is a 32 bit unsigned integer. The Mode 9 header contains the invocation counter. The T-mode and the C1 mode-messages use the same counter.

The counter is owned by the M-Bus device. Description and handling of the counter is specified in EN 13757-3 section 9.2.2. The counter is incremented for every new encrypted message. The M-Bus device is seen as a "restrictive system" to NOTE1 in section 9.2.2 of EN 13757-3, and therefore the counter will not wrap around beyond the maximum value of 0xFFFFFFFF; in that case the increment stops and the counter can no longer be used. The counter will be reset when the P2 User key changes.

The receiver of a message, either the E-meter or the M-Bus device, shall check the validity of the counter. The encrypted message is validated as follows:

1. the received counter must have a value that is max 100 higher than the previously validated counter;
2. the received message is encrypted and received correctly, i.e. checksum and other M-Bus fields are correct;
3. the message is decrypted and authenticated correctly.

Only encrypted messages that conform to this validation rule shall be accepted by the receiving M-Bus device. When the E-meter is the receiver of a message that doesn't pass the validation of the counter (step 1), the message is accepted and event 134 (M-Bus security error) is raised. The Invocation Counter of this message must be accepted.
Remark: the Invocation Counter must be stored in non-volatile memory (to prevent the reset of the counter in case of a power down of the E-meter).
Unencrypted messages (that use Security Mode 0) will not contain Invocation Counters.

An example of a sequence diagram for an M-Bus device is given in figure 5.

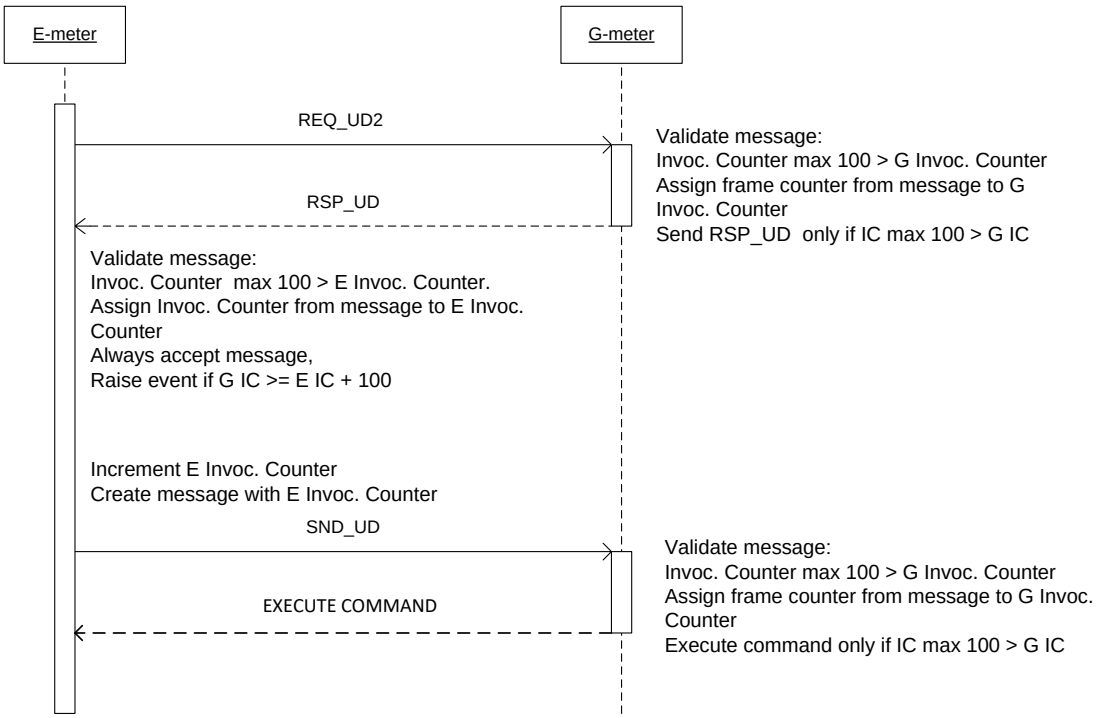


Figure 5: Handling of the Frame Counter

It is important to realize that the G-meter is the owner of the counter and the E-meter is merely using it:
The use of one counter owned by the Gas meter also facilitates easy exchange of E-meters.

Note : An efficient implementation of this protocol in the E-meter would probably predict the Invocation Counter and encrypt the messages to be sent to the M-Bus device before the hourly message from the M-Bus device is actually received. Synchronizing the time might require a more complex approach.

6APPLICATION LAYER

This part of the document describes the required M-Bus communication protocol between the residential electricity meter, functioning as M-Bus master, and M-Bus slave devices.

The installation part, such as the installation process of an external M-Bus device, removing an external M-Bus device, exchanging an external M-Bus device, is described in the separate document ‘uniform binding process’.
The application layer includes the data that is transmitted. For the M-Bus protocol the data structures and data types of the application layer are described in EN 13757-3.

6.1Meter Value Transfer

M-Bus devices can transfer 5 minutes and hourly values. In the hourly messages the current hourly value and the previous 3 hourly values including the M-Bus device time stamp of the last hourly value is transmitted. Every 5 minutes only the last stored 5 minute value and the appropriate timestamp is transmitted.
The M-Bus transfer will use the Storage Number bit in the DIF block to signify the stored values.

6.2Commands

6.2.1Set Date and Time Procedure

The M-Bus device has an internal clock and it should be synchronised by the E-meter.
Synchronisation is done:

- At every time change of the M-Bus Master
- Depending on the arrival time of the 5-minute value inside or outside the window where it is expected by the E-meter. See Use Case 13 in the Main Companion Standard for the details.

The maximum allowed clock deviation between E-meter and M-Bus device is 60 seconds. If the M-Bus device receives a new system time through the Set Date and Time mechanism then it verifies the difference between the new time and the old M-Bus Device system time. If the difference is more than 60 seconds then a “Clock synchronization error” is set (ref 6.3.3).
The M-Bus device will always set its system time to the time received in the synchronisation message. The time used in the P2 messages is UTC. Format Type I specified in EN 13757-3 is intended for local time but in this companion standard it shall be used for UTC[3]

The time is set using the following message with the special CI-code as in table 23:

Field	Hex	Remark
TC	00h	Set time

[3] The fields ”Second”, “Minute”, “Hour”, “Day”, “Month”, “Year”, “Day of Week”, “Week”, “Leap year” shall contain the UTC time. The fields “Time during daylight saving” and “Daylight saving deviation” may be set by the E-meter but shall be ignored by the M-Bus device. Example: UTC time 16 July 2013; 13:00 shall be coded as ”Second=0”, “Minute=0”, “Hour=13”, “Day=16”, “Month=7”, “Year=13”, “Day of Week=2”, “Week=0”, “Leap year=0”, “Time during daylight saving=0” and “Daylight saving deviation=0”.

Field	Hex	Remark
	xxh, xxh, xxh, xxh, xxh, xxh	New time in Format I (but used for UTC; see remark)
	00h,00h,00h	Reserved
	2Fh, 2Fh, 2Fh, 2Fh	Filler bytes

Table 23: Time set

6.2.2 Clearing the Status Word

The meaning of the Status bytes is described in table 25 in chapter 6.3.3.

The E-meter should clear the status bytes after each time an error is retrieved from the M-Bus device by sending:

Field	Hex	Remark
DIF	04h	32 bits
VIF	FDh	Use a VIFE
VIFE	97h	Error Flags
VIFE	06h	Clear the bits
Mask	xxh xxh xxh xxh	4 byte mask

Table 24: Clearing the Status Word

The mask contains the flag values that you want to reset and must be used for the corresponding error bits that are set.
Details can be found in EN 13757-3 chapter 8.

6.2.3 Set new key

The following keys can be set:

- User key
- firmware update authentication key

See chapter 6.5.1 for further description.

6.3Readout List

The read out list specifies which data blocks are sent by default.

Meter specific data blocks are defined in section 6.4. The order in which data blocks are inserted in an RSP_UD or SND_NR frame is not specified.

The following holds:

- Data Information Fields (DIF) and Value Information Fields (VIF) are mandatory and are coded as in EN 13757-3.
- Extended Data Information Fields (DIFE) and Extended Value Information Fields (VIFE) are mandatory to distinguish tariff based values or special units.

All types slave meter will send the data if not specifically polled for a specific data item as described per device- and message-type below:

For Gas meters (device type =03h) 4 different data messages (SND_NR) apply:

- 5 minutes data message.
  This message only contains the actual meter reading and timestamp according to chapter 4.3.3.

- Normal (short) hourly message.
  This message contains only the timestamp, last captured hourly value and 3 previous hourly values as described in chapter 6.4.4.1.

- Daily (long) hourly message
  This message contains:
  - 6.3.3 Status word
  - 6.4.1 Equipment identifier
  - 6.4.4.1 Timestamp, the last captured hourly value and 3 previous hourly values

- Push message
  This message contains:
  - 6.3.3 Status word
  - 6.4.1 Equipment identifier
  - 6.4.3 Actual timestamp without any hourly value

The readout list for the daily (long) hourly message is the default response on a REQ_UD2 or SND_UD2 request.

Thermal meters (device type =0 Dh) will send the following data items if not polled for a specific data item:

- Chapter 6.4.5 Thermal (heat / cold) Meter specific data blocks:
    - Hourly meter reading heat
    - Hourly meter reading cold

Water meters (device type = 07h) will send the following data items if not specifically polled for a specific data item:

- Chapter 6.4.6 Water Meter specific data blocks: Hourly Meter reading volume.

6.3.1 Changing the readout list

The readout list can be changed with a SND_UD2 within a FAC and data records containing the data field 1000b, which means “selection for readout request”. The following VIF defines the selected data as listed in EN 13757-3 and no data are transmitted. The answer data field is determined by the master. The slave can select several variables by sending more data blocks with this data field in the same telegram.

The actual values are retrieved by issuing a SND_UD2. The slave should restore the default readout list immediately after it retrieved the data..

When changing the readout list does not succeed the first time, a maximum of 2 retries should be performed.

6.3.2 Terminating the FAC

The FAC can be closed by sending a SND_NKE. The readout list is reset by terminating the FAC.

6.3.3Reading the Status word

The M-Bus device has a 32 bit status word. The status bits 0-19 are defined in table 25 below and are common for all M-Bus device vendors. The status bits 20-31 are vendor specific, see Annex D Vendor specific status bits.

Bit	Meaning with Bit set	Meaning with Bit not set	Push
0	Battery low	Battery not low	yes
1	Battery consumption high	Battery consumption not too high	yes
2	Reverse flow*	No Reverse flow	yes
3	Tamper P2	No Tamper P2	yes
4	Tamper P0	No Tamper P0	yes
5	Tamper case	No Tamper case	yes
6	Tamper magnetic	No Tamper magnetic	yes
7	Temp out of range	Temp not out of range	yes
8	Clock sync error	No Clock sync error	no
9	SW error	No SW error	yes
10	Watchdog error	No Watchdog error	yes
11	System/hw error	No System/hw error	yes
12	CFG Calibration error	No CFG Calibration error	yes
13	High Flow > Qmax	No High Flow > Qmax	no
14	Temp sensor error	No Temp sensor error	no
15	Binding flag**	No Binding flag	yes
16	FW update successful	No FW update performed	no
17	FW update unsuccessful	No FW update performed	yes
18	FUAK change successful	FUAK change unsuccessful	no
19	reserve	reserve	n/a
20-31	Vendor specific, see Annex D	Vendor specific, see Annex D	

* During the time that the flow streams in reverse direction the gas meter display will show the text: ‘Gas terug’.

** The binding flag is set by the M-Bus device when the device is in installation mode and it has been bound to an E-meter (it received the for this specific M-Bus device intended CNF_IR). When the M-Bus device is set in installation mode again and receives a CNF_IR from the same E-meter it will not set the binding flag again. The binding flag will only be set in case the CNF_IR is from another E-meter.

Table 25: Status Word

There is a distinction between normal errors and push errors (see Push column in the table above). Push errors will trigger an immediate and extra SND_NR push message (without opening a FAC) to be sent in order to inform the E-meter of the occurrence of the error/event.

Keep in mind that this push-message can be send within 100 ms by the G-meter, after occurence of the event. The E-meter has to switch from transmit to receiver mode as soon as possible to be able to handle this push-messages.
The E-meter can retrieve the status from the M-Bus device by sending the status information according to table 26:

Field	Hex	Remark
DIF	04h	32 bits
VIF	FDh	Use a VIFE
VIFE	17h	Error Flags

Table 26: Retrieve status

6.4 Variable Data Blocks

Note that all variable data blocks must be send encrypted when the User key is set (equivalent to the User key set to a non-zero value).
Variable data blocks of the C-mode messages containing measurement data shall be handled by the E-meter to be able to provide data for the P1 port.

6.4.1 Equipment Identifier

Field	Hex	Remark
DIF	0Dh	Variable length ASCII
VIF	78h	Equipment identifier
LVAR	11h	Length 17
	34h, 33h, 32h, 31h	Equipment identifier 17 ASCII, e.g. ABCD1234567891234
	39h, 38h, 37h	
	36h, 35h, 34h	
	33h, 32h, 31h	
	44h, 43h, 42h, 41h	

Table 27: Equipment Identifier

All meters are uniquely identified by a 17 ASCII character Equipment identifier.

Note : If the serial number is shorter than 10 characters, leading zeroes (coded as 30h) shall be added.

6.4.2 Remote read of firmware and hardware versions

The P2 interface must support remote reading of firmware and hardware versions. These VIF/VIFE's should not be added to the readout list by default. The master can add and remove these VIF/VIFE by issuing a 'selection for readout request'.

6.4.2.1 Detailed version info

The detailed version info is using the following VIF's (DIF = 08h):

VIF/VIFE = FDh 0Ch ("Model / Version"),
VIF/VIFE = FDh 0Dh ("Hardware version number") for the Hardware version,
VIF/VIFE = FDh 0Eh ("Metrology (firmware) version number"),
VIF/VIFE = FDh 0Fh ("Other firmware version number") for the firmware version.

To identify the various HW, FW and configuration versions, the M-Bus device shall use properties in the response string. A property is defined as "*name*=*value*".

The following properties are mandatory.

Type	VIFE			
	0Ch	0Dh	0Eh	0Fh
ESMR Protocol	ESMR=			
Metrology FW			met=	
Metrology HW		met=		
Communication FW				com=
Communication HW		com=		
Application FW				apl=
Application config				cfg=

Table 28: Detailed version info

Application configuration is used to identify a set of parameter values that determines the behaviour of the meter. These parameters are set during production of the meter. In the case that for a field no information is available, it is not allowed to leave this field empty (e.g. fill in "none").

Each property is to be terminated with CR/LF (ASCII characters <CR><LF>), also when multiple properties are combined in a single response.
Examples (actual text usage free to supplier):

VIF/VIFE = FDh 0Dh
Return value:
met=PCBx1.x2<CR><LF>
com=M-Bus module supplier<CR><LF>

VIF/VIFE = FDh 0Eh
Return value:
met=FW123.4.5<CR><LF>

6.4.3Time stamp

M-Bus devices transfer either 5 minute values or hourly values, either value will be accompanied with a time stamp of the moment the value is determined. The Storage Number bit in the DIF block of the time stamp signifies the hourly value. The time stamp is UTC and sent in Format I.

Field	Hex	Remark
DIF	46h	6 bytes integer, storage bit set
VIF	6Dh	Extended Date and Time compound data type I
	xxh, xxh, xxh, xxh, xxh, xxh	Date/Time (yy.mm.dd.hh:mm:ss)

Table 29: Time stamp 5 minute values

6.4.4Gas Meter specific data blocks

Gas Meter specific data blocks contain the Meter Reading temperature converted Volume.

6.4.4.1 For hourly messages:

There are 2 different types of hourly messages:

- Normal (short) hourly message: The Encrypted Variable Data Blocks (Records) contain only the Time stamp (ref section 6.4.3) and the Meter specific data blocks described in chapters 6.4.4 – 6.4.7.
- Daily (long) hourly messages: This message contains the data blocks of the short hourly meter data message but also the Status Word (see chapter 6.3) and Equipment ID (see chapter 6.4.1).

The hourly messages will transfer the hourly index plus the last 3 hourly values. In case the previous 3 hourly values are missing the 3 previous hourly values will be the same value as the current hourly value. This is done using the compact profile without registers. Absolute values are used so the separate base value record is not needed. A storage number of 8 is used, according to the M-Bus standard.
For Gas Meters G10-G25 the display is in 10 liter resolution, therefore separate VIFs are necessary.

Values used in the example below:

Time	Index Value
03:00	100.123
04:00	101.456
05:00	102.789
06:00	103.000

The timestamp record is modified to give the base time using storage # 8. Value =

Field	Hex	Remark
DIF	86h	6 bytes integer, extended
DIFE	04h	Storage # = 8
VIF	6Dh	Extended Date and Time compound data type I
Date/time	xxh	dd/mm/yy 02:00:00
	xxh	
	xxh	
	xxh	
	xxh	
	xxh	

Table 30: Time stamp hourly values

The Spacing Control byte is set as follows :-

Bits	Meaning	Value Used
0..3	Element size (low nibble of DIF)	8 digit BCD = 1100b
4..5	Spacing unit	Hours = 10b
6..7	Increment mode	Absolute value = 00b

Table 31: Spacing Control byte

Hence the value used is 00101100b = 2Ch. The corresponding spacing value is 1 (for 1 hour).

Field	Hex	Remark
DIF	8Dh	Variable length, extended
DIFE	04h	Storage # = 8
VIF	93h -or- 94h	93h for G4 and G6: Unit m^3, multiplier 0.001, extended -or- 94h for G10,G16 and G25: Unit m^3, multiplier 0.01, extended
VIFE	1Fh	Compact profile without registers
LVAR	12h	18 following bytes
Spacing Control	2Ch	8 digit BCD, hours, absolute value
Spacing Value	01h	1 hour
(Oldest) value 1	23h	100.123
	01h	
	10h	
	00h	
Value 2	56h	101.456
	14h	
	10h	
	00h	
Value 3	89h	102.789
	27h	
	10h	
	00h	
(Newest) value 4	00h	103.000
	30h	
	10h	
	00h	

Table 32: Daily short hourly Gas Meter message

6.4.4.2 Gas Meter specific data blocks for 5-minutes messages:

Field	Hex	Remark
DIF	4Ch	8 digit BCD
VIF	13h -or- 14h-	13h for G4 and G6: Multiplier 0.001; Unit m^3 -or- 14h for G10, G16 and G25: Multiplier 0.01; Unit m^3
Value	34h	1.234 m^3
	12h	
	00h	
	00h	

Table 33: 5 minute Gas Meter message specific data blocks

6.4.5Thermal (heat / cold) Meter specific data blocks for 5 min. and hourly values

To differentiate between Heat and Cooling values the Device Unit in the DIFE field is used. For Cooling values the Device bit is set to TRUE. For Heat values the DIFE field is omitted or the Device bit in the DIFE is set to FALSE.

Meter Reading Energy Heat

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set)
VIF	0Fh	Scaler 7; unit J (0,01 GJ)
	27h	Meter reading, e.g. 03141,27 GJ
	41h	
	31h	
	00h	

Table 34: Meter Reading Energy Heat specific data blocks

Meter Reading Energy Cold

Field	Hex	Remark
DIF	CCh	8 digit BCD (storage bit is set)
DIFE	40h	Cooling unit
VIF	0Fh	Scaler 7; unit J (0,01 GJ)
	27h	Meter reading, e.g. 03141,27 GJ
	41h	
	31h	
	00h	

Table 35: Meter Reading Energy Cold specific data blocks

6.4.6Water Meter specific data blocks for 5 min. and hourly messages

Meter Reading Volume- **Field**	**Hex**	**Remark**
DIF	4Ch	8 digit BCD (storage bit is set)
VIF	13h	Multiplier 0,001; unit m³
	74h	Meter reading, e.g. 03141,274 m³
	12h	
	14h	
	03h	

Table 39: Meter Reading Water Meter volume specific data blocks

6.4.7Slave E-Meter specific data blocks for 5 min. and hourly messages

Meter Reading- **Field**	**Hex**	**Remark**
DIF	4Ch	8 digit BCD (storage bit is set)
VIF	03h	Multiplier 1; unit Wh
	74h	Meter reading, e.g. 03141274 Wh
	12h	
	14h	
	03h	

Table 40: Meter Reading Slave E-Meter specific data blocks

6.5Key Management Procedures

Every M-Bus device is configured by the supplier with a Default key and Firmware update authentication key. The supplier guarantees that these keys are unique for every meter. These keys are registered in a shipment file with the device's Equipment Identifier (ref 6.4.1) or Short ID (ref 4.2.2). The value of the keys cannot be deducted from any combination of the values of the attributes of the M-Bus device (the keys are chosen randomly). The Default key is used exclusively to decrypt every new User key and Firmware update authentication key that is received over the M-Bus. The Default key will never be renewed.

The User key is used to encrypt all messages. The User key is transferred to the E- meter over P3 and the same key is, encrypted with the M-Bus devices Default key, transferred to the E-meter and from there it is transferred to the M-Bus device as described in section 6.5.1.

The firmware image signature key is the public key used to check the firmware signature. The M-Bus device meter vendor signs the firmware image. This signature for the firmware uses a strong hashing algorithm (SHA 2 family) and signs the result using an asymmetric key pair and appends the result to the firmware image so that it can be checked by the M-Bus device using the public key.
The algorithms and key sizes used are SHA256 for hash and ECDSA with a key set from the ecp256r1 curve.

The firmware update authentication key can be changed by the CS via the E-meter using the Key Exchange Procedure, see section 6.5.1.

Note that key changes can occur at any time during the operation of the M-Bus devices. Note that with ALL key changes the M-Bus device receives the new key encrypted with the device's default key.

6.5.1 Key Exchange Procedures

After installation the M-Bus device sends meter reading data. These transmissions contain the unencrypted Short ID and meter reading data. The electricity meter will make this Equipment identifier available to the CS.
The CS will transfer a key for the M-Bus device through the (encrypted) P3 channel to the Electricity meter. The purpose is to transfer the key into the M-Bus device. The key is transferred encrypted and authenticated with the Default key and the CS performs this encryption.

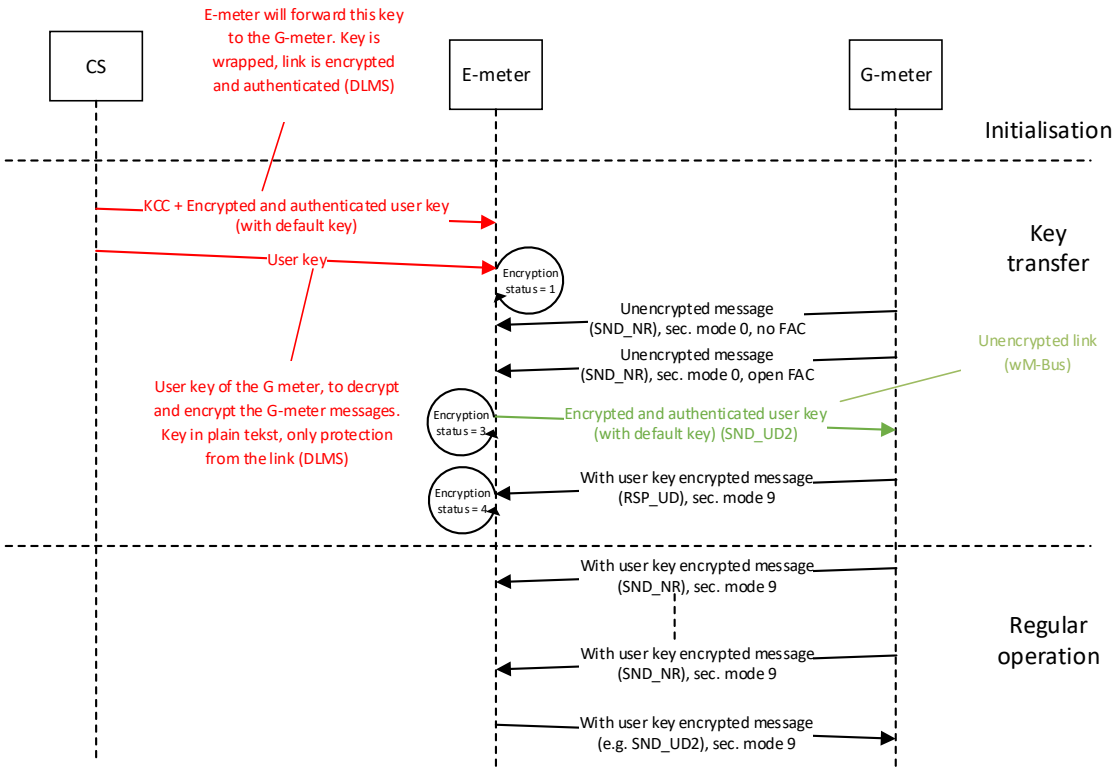


Figure 6: Key Exchange Procedure (example for User key)

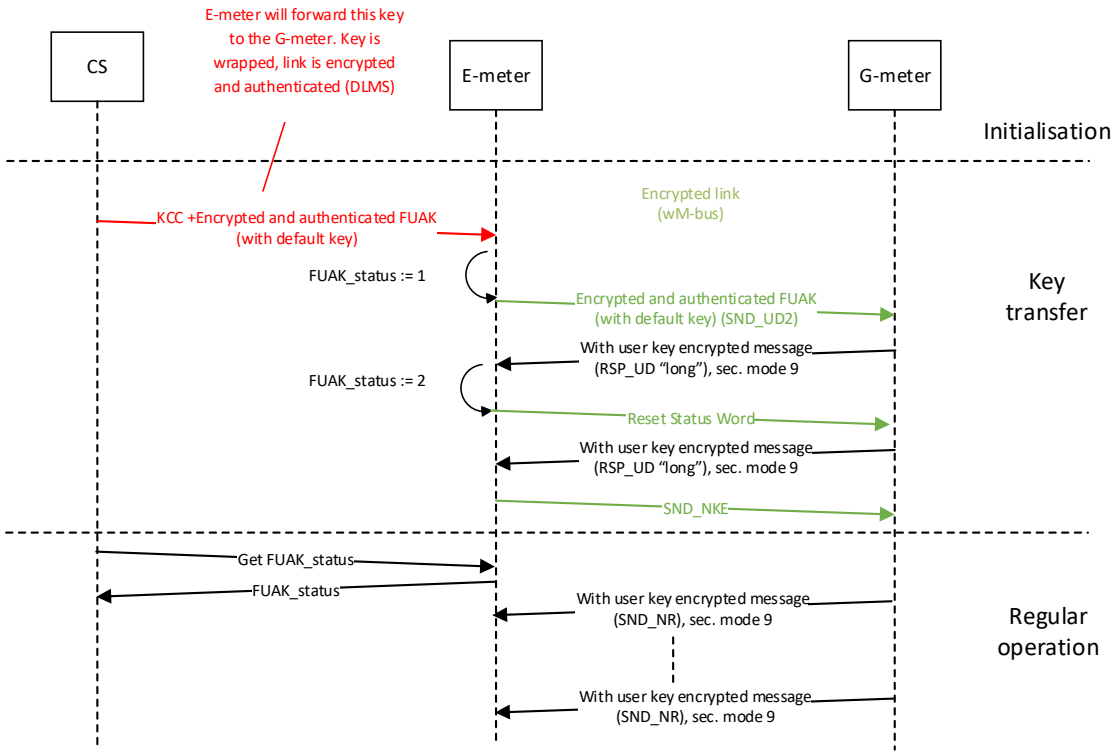


Figure 6a: Key Exchange Procedure (example for FUAK key)

User keys are transferred through P3 as plain octet string, for use in the electricity meter, and as octet string encrypted and authenticated with the M-Bus device's Default key. The encrypted and authenticated string is transferred over the P2 interface, using an unencrypted message type. This is a deviation from DLMS Blue Book, where only the first key update is unencrypted. All subsequent updates on DLMS are encrypted with the user key. On M-Bus level however, all key updates are sent with unencrypted M-Bus messages. This has the advantage that key updates are still possible even when the current user key is lost and/or the invocation counter is exhausted.

Also the Firmware update authentication key in the M-Bus device may be changed with this procedure. The difference is that in these cases the key will not be made known to the Electricity meter. Also the key-ID will have value 1 instead of 0 in that case.

It is not possible to update the Firmware Image Signature Key.

The CS stores and maintains one individual Key Change Counter (KCC) for each M-Bus device. The KCC is only used for key exchange and not for any other purpose, and not to be combined with any other counter. Each M-Bus device has one KCC to be used for all key changes.

The Key data consists of the key-ID (1 byte), the size of the key (1 byte) and the (value of) the key. This key data is encrypted with the default key of the M-Bus device using GCM with the Key Change Counter used as invocation counter. The GCM authentication tag is also produced. The Key Change Counter value must increment from previous value (checked at the gas meter). Per key exchange message only one key can be exchanged.

Note: in order to prevent the Central System and M-Bus device getting out of sync or Central System losing the Key Change Counter the following applies:

The Key Change Counter must be available and stored in the Central System. As standard procedure, the CS must use the amount of seconds counted from 1 January 2000. All M-Bus devices have their own, independent KCC which is initiated with value "0".

The values for key-ID are defined in table 43:

Value	Description
0	User key
1	Firmware update authentication key
2	reserved
3	reserved

Table 43: Key ID Definitions

The key data is arranged in a buffer as shown in figure 7. This is encrypted and authenticated using the meter's default key and the key change counter replacing the invocation counter in the IV. The IV has the same structure as used in normal Security Mode 9. A GCM authentication tag length of 8 bytes is used.

Key id (1byte)	Key size in bytes (1byte)	Key value ('size' bytes)

↓

Encrypted Key data (2 + 'size' bytes)	GMAC (8 bytes)

Figure 7: Encryption and Authentication of Key Data

This encrypted data plus the GCM authentication tag are sent in a variable length record. This record and a record containing the KCC are sent together to the meter in an unencrypted SND_UD2 command. See table 44.

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	True VIF is given in table 28 (of EN 13757-3)
VIFE	19h	Security key
LVAR	00h-BFh	Length including counter, key & tag.
Key Change Counter	KCC0	32-bit integer counter value where KCC0 is the MSB of the counter
	KCC1	
	KCC2	
	KCC3	
Encrypted key data	EKD0	Key ID
	…	Key Size
		AES KEY 1 (MSB)
	EKDN	AES KEY N (LSB)
GCM authentication tag	AT0	GCM authentication tag where AT0 is the MSB of the GMAC
	…	
	AT7	

Table 44: Key Change - user key

The M-Bus device will first check that the KCC is greater than the last one used. Verification of the counter is not time based. The meter simply checks whether the received counter is greater than the previous valid value. If the verification is successful, the data in the second record is decrypted and the GCM authentication tag is checked and validated. If successful and the key ID and size are valid, the key is accepted. The stored KCC is then updated. The response will indicate if the key was accepted or not.

The response to this message is a RSP_UD.

6.5.2Key Management Requirements and encryption requirements

Both the Default Key and the currently in use User key are to be registered in the back office. All keys are expected to be unique for every individual meter.

All wireless M-Bus devices will be delivered from the factory unencrypted (messages are sent using security Mode 0; unencrypted messages). Once the user key is set, all messages send by a G-meter should use security Mode 9.
Only key change messages and confirmation of installation request messages are always sent unencrypted by an E-meter. A time set command by an E-meter is sent unencrypted until the first user key is set. From that point in time, for a time set the same applies as for all other control commands: they must be sent with security Mode 9 only (a command that is sent with security Mode 0 will be ignored once the user key is set).

Notice that in some specific situations (e.g. after an E-meter replacement) the User key may not be available in the E-meter yet. However, the unencrypted headers of the M-Bus transmissions contain sufficient information (Short ID) for the initial installation process (binding process).

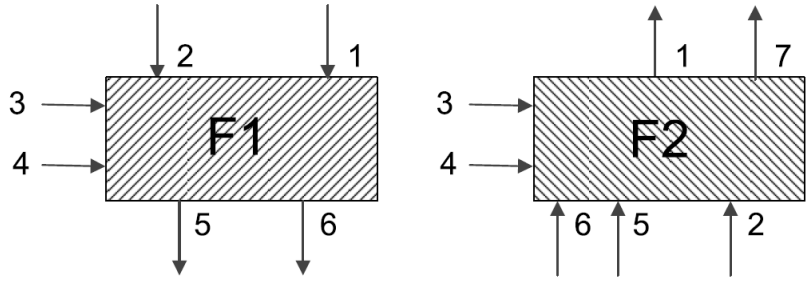
An overview of allowed M-Bus message types is listed below:

	ELL	Unencrypted	Encrypted		
		Allowed	Allowed	encryption	authentication
Message					
SND_NKE	No	Yes	Yes	No	Yes
ACK	Yes	Yes	Yes	No	Yes
SND_IR	Yes	Yes	Yes	Yes	Yes
SND_NR	Yes	Yes	Yes	Yes	Yes
SND_UD time	No	Yes	Yes	Yes	Yes
SND_UD2 reset status word	No	No	Yes	Yes	Yes
SND_UD2 key	No	Yes	No	---	---
SND_UD2 FUAK	No	Yes	No	---	---
SND_UD2 FW	No	No	Yes	Yes	Yes
REQ_UD2	No	Yes	Yes	No	Yes
RSP_UD normal	Yes	Yes	Yes	Yes	Yes
RSP_UD Change Readout	Yes	No	Yes	Yes	Yes
RSP_UD FW	Yes	No	Yes	Yes	Yes
CNF-IR	No	Yes	No	---	---
SND_NR C-mode (5 min.)	No	Yes	Yes	Yes	Yes

6.5.3Security mode 9 and AES-GCM as its encryption mechanism

The security mode 9 uses AES-GCM as its encryption algorithm. Details can be found in EN 13757-3, chapter 9.4.6.

AES-GCM takes four inputs: the plaintext (data to encrypt), the data to authenticate only, the key and the Initialization Vector (IV). There are two outputs: the cipher text (encrypted data) and the Authentication Tag.



Where:
F1 AES Galois/Counter Mode authenticated encryption function
F2 AES Galois/Counter Mode authenticated decryption function
1 plaintext (data to encrypt)
2 data to authenticate
3 key
4 initialization vector
5 encrypted data
6 authentication tag
7 fail, special error code

Function F1 is used by the sender of the message to encrypt and/or authenticate a message. The three ways in which function F1 can be used are:

Method	Input	Output
Encryption only	1 (plain text) + 3 (key) + 4 (IV)	5 (encrypted data)
Authentication only	2 (data to authenticate) + 3 (key) + 4 (IV)	6 (authentication tag)
Encryption and authentication	1 (plain text) + 2 (data to authenticate) + 3 (key) + 4 (IV)	5 (encrypted data) + 6 (authentication tag)

If there is no plaintext (data to encrypt), only the Data to authenticate (2) is used: for example in an ACK message. As defined in the EN 13757-3 (paragraph 9.4.6.3), the data to authenticate only is a concatenation of the fields Configuration Field, Length U, Length E and the unencrypted data in that case.

Corresponding the F2 function is used by the receiver of a message. The three ways in which the function F2 should be used are as follows:

Method	Input	Output
Encryption only	5 (encrypted data) + 3 (key) + 4 (IV)	1 (plain text)
Authentication only	2 (data to authenticate) + 6 (authentication tag) + 3 (key) + 4 (IV)	No output but authenticity confirmed
Encryption and authentication	5 (encrypted data) + 2 (data to authenticate) + 6 (authentication tag) + 3 (key) + 4 (IV)	1 (plain text) + authenticity confirmed

7FIRMWARE UPDATE

In total 3 security keys are directly involved in the firmware update process:

- The default key is used to update keys (the Firmware update authentication key can be updated). The default key is known in the CS and by the M-Bus device.
- The Firmware update authentication key is used by the CS to generate a MAC to protect the firmware and the header. It is known in the CS and by the M-Bus device.
- The Firmware image signature key is a asymmetric key pair used for creating a signature for the firmware (non repudiation). It consists of a private part (known only by the M-Bus device manufacturer) and a public part. This key is not updateable.
  This key is used in the CS to verify the digital signature and in the M-Bus device itself, to verify the digital signature of the firmware.

For normal data exchanges the user key is used to encrypt the data. The user key can be updated via the key exchange procedure (see chapter 6.5.1).

7.1 End to end overview

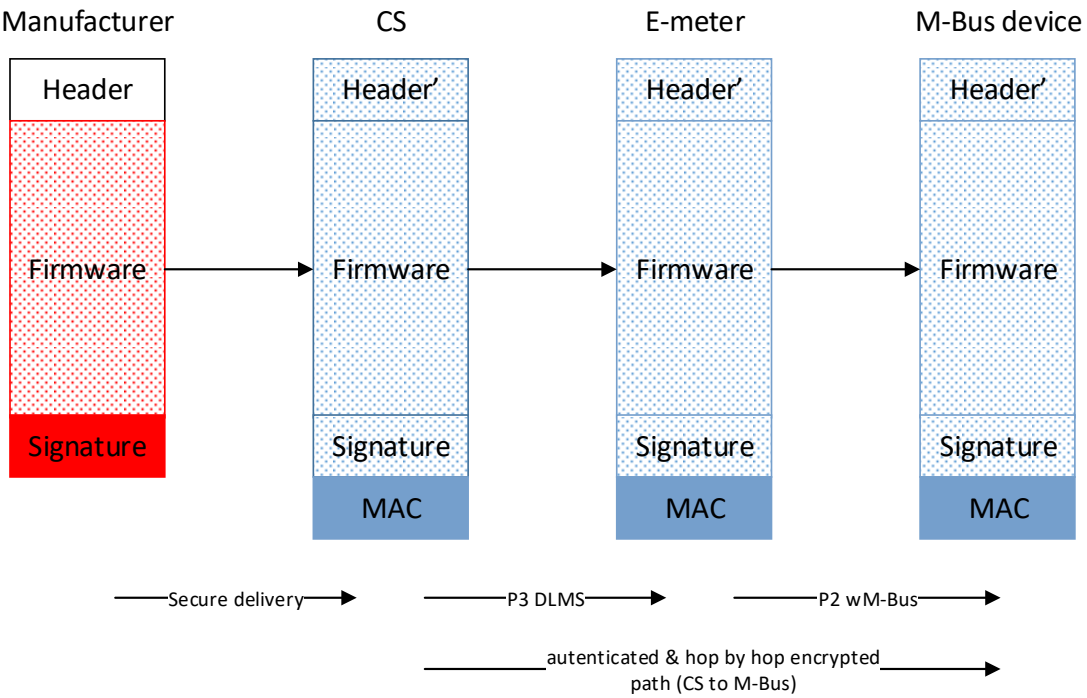


Figure 8: Firmware upgrade 'end to end'

The basic idea behind the process is that a manufacturer signed Firmware upgrade image is delivered to the Central System (CS in the figures) of the Grid Operator for further distribution through the communication network towards the M-Bus device.

The Firmware upgrade image will have a header describing certain properties of the Firmware upgrade image and allows the Grid Operator to implicitly set certain properties (like activation time, which will create a header') it wants to impose on the Firmware upgrade image to be executed by the M-Bus device.

The header properties are strictly to be used by the M-Bus device and should not be parsed or changed by any hops in the communication path from CS to M-Bus device.

The Grid Operator will authenticate the origination of the Firmware upgrade image and the properties set in the Firmware upgrade image header.

The firmware is signed with a Firmware image signature key. This key consists of a private part and a public part and is not updateable. The private part is owned by the M-Bus device manufacturer only and is used to create a firmware digital signature. The public part is used by the CS and the M-Bus device to verify the firmware digital signature.

A MAC is generated by the CS to protect the firmware upgrade by adding encryption of the firmware and it protects against manipulation of the header'. For generating this MAC the Firmware update authentication key is used.

The Firmware upgrade image is then transferred in smaller chunks from the CS via the DLMS protocol to an E-meter and from there to an M-Bus device using the M-Bus application layer protocol.

7.2Manufacturer to M-Bus device view

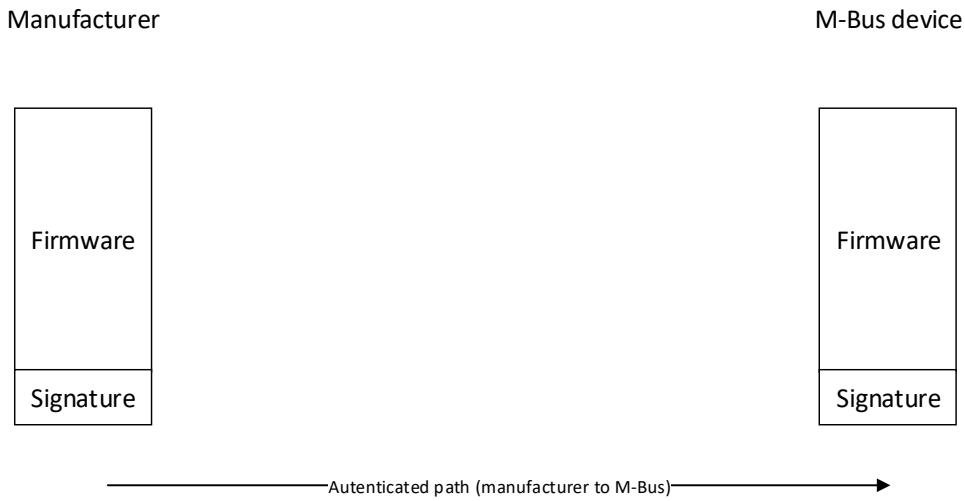


Figure 9: Firmware upgrade Manufacturer to M-Bus device

The previous described signing of the Firmware is to be able to check the integrity, authenticity and the origin of the Firmware from manufacturer to M-Bus device.

7.2.1Manufacturer to CS view

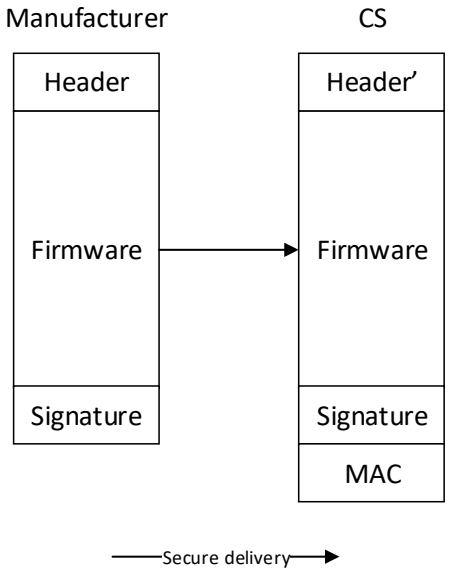


Figure 10: Firmware upgrade Manufacturer to CS

The manufacturer will deliver a generic Firmware to the CS with a standard header. It is up to the CS to change the header as needed on a per M-Bus device basis, or leave it as delivered. The Firmware is generic for all of the Meters from the manufacturer as specified in the header (manufacturer ID, Version number and type), it is up to the CS to authenticate the header as well as the Firmware on a per meter basis.
The CS will have to have functionality to access and store the unique M-Bus device “Firmware update authentication key” and the “Firmware image signature key”.

7.2.2CS to M-Bus device view

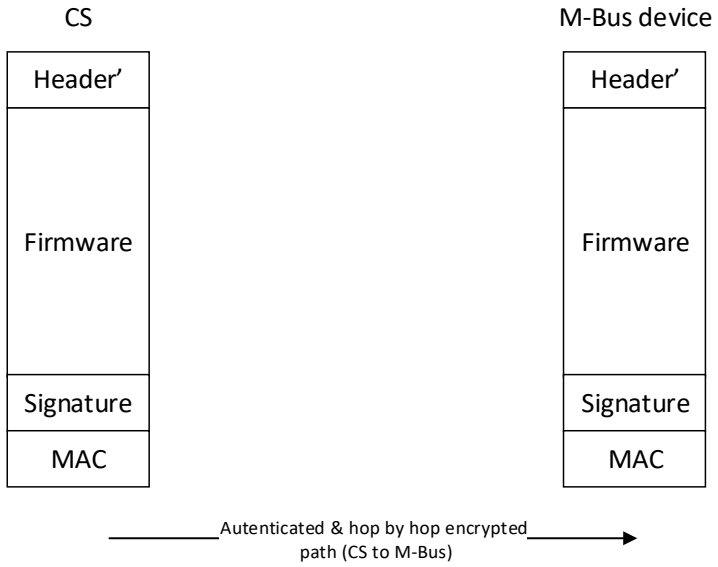


Figure 11: Firmware upgrade CS to M-Bus device

The firmware update authentication key is a key that is unique for every M-Bus device. The key is used to validate the authentication of the new M-Bus device firmware. The CS adds a MAC to the firmware image. The MAC is generated with the GMAC algorithm using the Firmware update authentication key. The M-bus device checks the MAC for the authenticity of the firmware. The initialisation vector (IV) to be applied uses the mode 9 structure, with the amount of seconds counted from 1 January 2000 as the variable element.

MS Byte	11	10	9	8	7	6	5	4	3	2	LS Byte
ID (LSB)	..	..	ID (MSB)	MFT (LSB)	MFT (MSB)	Ver-sion	Dev. type	CNT (MSB)	..	..	CNT (LSB)

Where:

- ID is the Identification number of the M-Bus device
- MFT is the Manufacturer ID
- Version is as per M-Bus header Version
- Dev. type is the device type as per M-Bus header (e.g. 03 for gas)
- CNT is the Invocation Counter of the IV (the amount of seconds counted from 1 January 2000

Note: the byte order of the IV is as described in chapter 5.3.

Figure 12: IV GMAC algorithm

7.2.3CS to E-Meter view

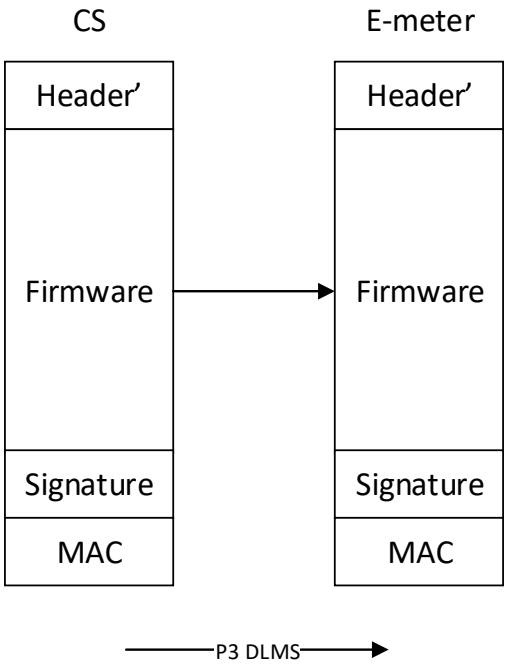


Figure 13: Firmware upgrade CS to E-Meter

From the CS to the E-meter DLMS must be used. To make the impact for the DLMS and P3 Specification minimal, the image transfer mechanism of DLMS is chosen.
See the ESMR P3 Companion Standard and the DLMS Blue Book. The Firmware upgrade image for the M-Bus device is at this stage nothing more than a block of data that needs to be transferred in the least obtrusive and most optimal way.
The transport of the Firmware upgrade image will use “store and forward” from CS to E-Meter, where the Firmware upgrade image will be buffered until the M-Bus device is available.
The “DLMS_image_transfer_initiate” call will carry the M-Bus address information that identifies for which M-Bus device the Firmware upgrade image is intended.
The interaction steps between CS and E-meter is further detailed in the Firmware update flow charts Appendix E.
The mapping between DLMS “image transfer” and P2 messages is given in Appendix A and the needed P2 messages will be described in chapter 7.3

7.2.4E-Meter to M-Bus device view

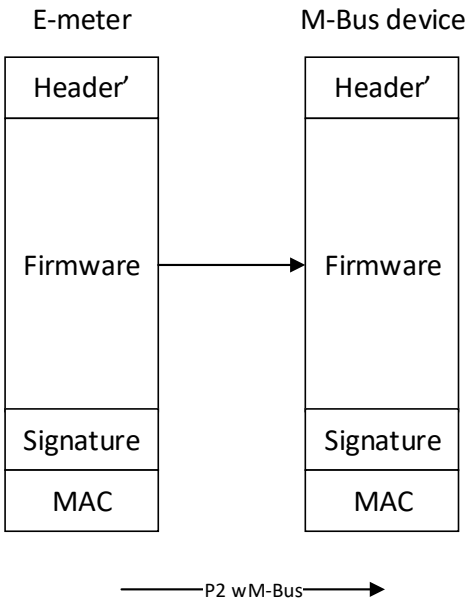


Figure 14: Firmware upgrade E-meter to M-Bus device

For this interface, wireless M-Bus with mode 9 security must be used. The mapping between DLMS 'image transfer' and P2 messages is given in Appendix A and the P2 messages themselves are found in chapter 7.3.
The central message for the P2 interface is the 'firmware upgrade status report' message. This message contains the 'Update state' and 'Error code' fields. With these fields the status and the state of the firmware update process can be determined at any moment and if needed reported to the CS.
The function 'Firmware upgrade request block status' is a function to check for image completeness, it is there to allow for both multicast and DLMS to P2 mapping completeness.
More detailed information about the interaction between CS, E-meter and M-Bus device during a successful Firmware update process can be found in Firmware update flow charts in Appendix E.

7.3 Firmware upgrade image structure

The firmware upgrade image structure is defined in a standard way for all M-Bus device manufacturers.

The three sections of the firmware upgrade image are shown in table 45. The first part of the header is fixed so that the start of the other sections can be identified.

Section	Length	Description
Header	Variable	Identifies firmware upgrade image, manufacturer, device it is intended for and size of other sections
Firmware image	Variable	The Firmware image itself, the manufacturer is completely responsible for its content. It can have an extra header, consist of several sub images or can be an incremental firmware update image. It can be optionally compressed and encrypted. It will have to support an authentication mechanism.
Security section (MAC from CS to MBUS device in ESMR5)	Variable	Information used for authentication and verification of the firmware upgrade image from CS to M-BUS device.

Table 45: Firmware upgrade image structure

The actual firmware image transferred is of course device and manufacturer specific.

7.3.1 Header Section

The header structure is shown in table 46. The header version and length fields allows additional fields to be added in the future without affecting the ability of older meters to use the same firmware upgrade mechanism.

Field	Type	Description	Remark
Firmware image magic number	4 bytes	Identifies a Firmware upgrade image as a Firmware image.	Fixed in Header
Header version	1 byte	Identifies the Version.	Fixed in Header
Header length	2 bytes	Total length of the header section.	Fixed in Header
Firmware image Version	4 bytes	Number of seconds since January 1, 2000 (Bit order equal to IV in 7.2.2)	Not fixed in Header' because we have to be able to send the same firmware version again in case of a failure
Firmware image length	4 bytes	Total length of the Firmware image section.	Fixed in Header
Security length	2 bytes	Total length of the security section.	16 bytes. Fixed in header
Security type	1 byte	Type of the security section (see table 47).	GMAC. Fixed in Header
Address length	1 byte	Length of the address field.	8 bytes length. Fixed in Header

Address type	1 byte	Type of the address field(see table 48).	M-Buss address. Fixed in Header
Address field	'Address length' bytes.	Specific address or wildcard address.	Man ID, Serial number, version, device type. Not fixed in Header'. Length is fixed, content dynamic.
Activation type	1	How to activate the firmware (see table 49).	Not fixed in Header'
Activation time	6 bytes	Time in format I. Used if activation type is 'timed activation'.	If activation type is not 2, then the content must be FFFFFF. Not fixed in Header'

Table 46: Header section

The 'security type' field defines what it is in the security section of the firmware upgrade image. For ESMR5 only option 2, GMAC is allowed and security length of 16 bytes.

Type	Description
0	No security.
1	SHA-256 hash
2	GMAC (preferred in NL)
3	CMAC
4	HMAC
5	ECDSA
6	...

Table 47: Security types

The 'address type' field defines what it is in the 'Address field' of the firmware upgrade image header, for now only 'MBUS address' is defined. The address itself will consist of 8 bytes consisting of the 'Manufacturer ID', 'MBUS device serial number', 'version' and 'device type'. The coding is according to the EN 13757-4 transport layer.

Value	Sub system type
1	MBUS address (wild cards allowed).
2	…

Table 48: Address types

The 'activation type' field defines how the firmware upgrade is activated by the MBUS device.

Value	Sub system type
1	Immediate activation
2	Timed activation[4]
3	Master initiated activation (by 'firmware up-

[4] In case the activation time is in the past, the firmware must be activated immediately.

	grade activate' com-mand).
..	..

Table 49: Activation types

7.3.2 Firmware upgrade states

The following states are defined in the firmware upgrade process:

Value	Description
0	IDLE state
1	DATA RECEIVE state
2	VALIDATING state
3	VALIDATED state
4	VALIDATION failed state
5	ACTIVATING state
6	ACTIVATED state
7	ACTIVATION failed state

Table 50: Firmware upgrade states

7.3.3 General structure of used VIB codes

The firmware upgrade process is using the following general VIB:

Code	Meaning
0Dh	DIF variable data
FDh	First extension table of VIF codes
F7h	First free (reserved) VIF code 0x77
XXh	VIF firmware sub codes
YYh	LVAR
0..n	Data

Table 51: General VIB

The following firmware sub codes are defined:

REQUEST		RESPONSE	
Code	**Meaning**	**Code**	**Meaning**
	SND_UD2		RSP_UD
30h	Firmware upgrade start	31h	Firmware upgrade status report
32h	Firmware upgrade send data	31h	Firmware upgrade status report
33h	Firmware upgrade validate	31h	Firmware upgrade status report
34h	Firmware upgrade activate	31h	Firmware upgrade status report
35h	Firmware upgrade cancel	31h	Firmware upgrade status report
	Request for readout		
31h	Firmware upgrade request status	31h	Firmware upgrade status report
36h	Firmware upgrade request block status	36h	Firmware upgrade block status report

Table 52: Firmware upgrade sub codes

7.3.4 Firmware upgrade messages

All firmware upgrade messages are sent with the SND_UD2 primitive. The SND_UD2 primitive consists of a SND_UD with an automatic implied REQ_UD2. The response to a REQ_UD2 is the default active readout list. In order for the Firmware messages to report a "Firmware upgrade status report" to a SND_UD2, it needs to be specifically made the default readout list by sending a "Firmware upgrade request status". After that, all firmware upgrade messages (except for firmware update request block status message) will return a 'Firmware upgrade status report'.

Remark:
The E-meter must not check the first received Firmware upgrade status report from the G-meter.

7.3.5 Firmware upgrade status report response

The firmware upgrade status report is defined as follows:

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	First extension table of VIF codes
VIFE	F7h	First free (reserved) VIF code 77h
VIFE	31h	Firmware upgrade status report
LVAR	NN	Length
Update State	1 byte	Enumeration, see table 50
Error code	1 byte	Enumeration, see table 54
Agreed block size	1 byte	Size of a transfer block. If error code = 1, this is the max block size supported by the M-Bus device. Remark: The E-meter must be able to handle a max block size of 177 bytes (origin: max size of P2 telegram is 255 bytes minus overhead). See P3 Companion Standard chapter 5.12.2 for the maximum number of bytes that can be transferred.
Validation field length	1 byte	Specifies the length of the validation field. Length can be 0.
Validation field	'Validation field length' bytes.	When 'Update state' is VALIDATED, this field will contain the verification data that can be reported back in the DLMS 'image_to_activate' field.

Table 53: Firmware upgrade status report

The following error codes have been defined:

Code	Meaning
0	No error
1	Block size (application layer) not sup-

	ported
2	Image size too big
3	Invalid block number
4	Data receive error
5	Image not complete error
6	Invalid security (error)
7	Invalid firmware for this M-Bus device
8	Signature error
9	MAC error
10	Corrupt header
	…

Table 54: Error codes

Note:
After an error (except code 0 (no error), 1 (block size not supported) and 5 (image not complete)) occurs, the error is repeated untill the FAC times out. Reason for this is to save the battery.
At error code 1, the E meter must continue (and adapt the block size to the block size of the G meter).
At error code 5, the E meter must request the block status
report to find out which blocks are missing.

7.3.6 The firmware update request block status

The firmware update request block status message returns a firmware update block status report which is defined as follows:

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	
VIFE	F7h	
VIFE	36h	Firmware upgrade block status report
LVAR	NN	Length
Block status	NN bytes	Array of bits, one for each block, bit is set if block transferred. Bit is reset if block is not transferred.

Table 55: Firmware update block status report

7.3.7 Firmware upgrade start

The ‘firmware upgrade start’ message will bring the M-Bus device in a state where it is allowed to be more responsive (enabling more FAC cycles than during normal operation) on the P2. Since the firmware messages are protected with mode 9 security it is difficult to exploit this feature for exhausting the battery. It is up to a manufacturer to take additional

measures for this. The ‘firmware upgrade start’ message will make the needed resource reservations to perform a firmware update. It is also used to request and negotiate a ‘block size’ for the subsequent ‘firmware upgrade send data’ messages.

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	
VIFE	F7h	Firmware function
VIFE	30h	Firmware upgrade start
LVAR	NN	Length of the variable data.
Bytes to transfer	4 bytes	Length of the complete image
Block size	1 byte	Requested block size. Check the status report for the ‘negotiated’ block size.

Table 56: Firmware upgrade start

7.3.8 Firmware upgrade send data

The ‘firmware upgrade send data’ message is used to transfer a ‘block’ of negotiated ‘block size’ firmware data.

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	
VIFE	F7h	Firmware function
VIFE	32h	Firmware upgrade send data
LVAR	NN	Length of the variable data. Data length is this value - 2
Block number	BN0	Block number in firmware upgrade image. First block number starts with 00h
	BN1	
Data	XX	Data byte 1
	XX	Data byte n

Table 57: Firmware upgrade send data

7.3.9 Firmware upgrade validate

The ‘firmware upgrade validate’ message will start the validation process of the received firmware. MAC and digital signature will be checked.

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	
VIFE	F7h	Firmware function
VIFE	33h	Firmware upgrade validate
LVAR	00h	Length

Table 58: Firmware upgrade validate

In the case of a time based activation, just before the activation itself, an additional validate must be performed to check whether the firmware has not been altered during storage.

7.3.10 Firmware upgrade activate

The ‘firmware upgrade activate’ message is used to activate a firmware on command.

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	
VIFE	F7h	Firmware function
VIFE	34h	Firmware upgrade activate
LVAR	00h	Length

Table 59: Firmware upgrade activate

7.3.11 Firmware upgrade cancel

The ‘firmware upgrade cancel’ message can be used to release the resources reserved by the ‘firmware upgrade start’ message.

Field	Hex	Description
DIF	0Dh	Variable length
VIF	FDh	
VIFE	F7h	Firmware function
VIFE	35h	Firmware upgrade cancel
LVAR	00h	Length

Table 60: Firmware upgrade cancel

7.3.12 Firmware upgrade request status report

This message is a ‘request for readout’. At any moment the status and state of the firmware upgrade process can be requested.

Field	Hex	Description
DIF	08h	Select for readout
VIF	FDh	
VIFE	F7h	
VIFE	31h	Upgrade request status report

Table 61: Firmware upgrade request status report

7.3.13 Firmware upgrade request block status

This message is a ‘request for readout’. At any moment the block status can be requested.

Field	Hex	Description
DIF	08h	Select for readout
VIF	FDh	
VIFE	F7h	
VIFE	36h	Upgrade transfer block status

Table 62: Firmware upgrade request block status

NOTE:
After activation of the new Firmware the M-Bus device shall immediately send an SND_NR message with the daily long readout list. With immediately is meant directly after activating the new firmware the SND_NR message with the daily long readout list will be send and not at the next scheduled time when this message will be send (00:00 h)

During the Firmware update process (including validating/activating of the firmware) the regular interval data messages for 5-min an hourly values may be temporarily halted, with a maximum of 12 times a 5-min C-mode message and 1 hourly T-mode message missing.

The next Firmware update process (continuation if the update has not completed within 1 hour) can take place 24h later, at the first availability of the FAC.

7.3.14 Reboot of the E-meter

Reboot of the E-meter before sending first block:
The complete firmware upgrade is restarted (firmware upgrade request status again, firmware upgrade start, and so on).

Reboot of the E-meter during blocks transfer:
After the reboot the E-meter should
1) send the firmware upgrade request block status (Chapter 7.3.13),
2) ask for the firmware upgrade request status report (Chapter 7.3.12) and then
3) send next block.

Reboot of the E-meter after sending all the blocks, but before firmware upgrade validate request:
After reboot the meter should
1) send the firmware upgrade request block status (Chapter 7.3.13),
2) ask for the firmware upgrade request status report (Chapter 7.3.12) and then
3) validate.

8POWER SUPPLY

8.1Power outage

Wireless devices need not necessarily detect power failures of the E-meter and the connected communication device. The meter reading that is registered, the meter reading that is sent to the E-meter and the meter reading on the meter's display should be consistent at all times. The meter reading that is sent to the E-meter and the meter reading on the display of the M-Bus device must have the same value at the time the meter reading is stored (for an hourly value this is the value at exactly XXh:00m:00s every hour). Because of the randomisation interval this value will be sent later. Any registered interval data may be lost during power outage.

When the E-meter has scheduled a message for the G-meter before a power down (during which the E-meter lost its date and time), messages for the G-meter can be deleted.

9INSTALLATION PROCEDURES

The flowchart for entering the different modes in the G-meter is described in Appendix C. The operation of the devices is described in the document ‘Uniform binding process [6]’. This document focusses on the M-Bus protocol for the binding process.

9.1General installation procedures

During installation the M-Bus devices will be registered by the E-meter.

The installation mode of the E-meter can be activated as described in the ‘Uniform binding process [6]’. The E-meter always accepts and processes installation mode requests (SND_IR) from wireless M-Bus devices which have a value in the version field equal to 50h or higher (EMSR version). When the E-meter is in Installation mode it is able to select the M-Bus device to be bonded to. If the value in the version field is lower than 50h, the serial number will not be shown in the display of the E-meter and binding is not possible in that case.

After the M-Bus devices are registered in the E-meter and M-Bus devices are in Customer mode (as described in section 9.2), several administrative tasks shall be executed. The User keys need to be transferred before the readout list is changed. The readout list is changed to read out the firmware and hardware versions during the installation procedure. The standard readout list is activated by sending a SND_NKE.

For identification of the M-Bus devices in the E-meter as well as in the back office, the Short ID shall be used.

9.2M-Bus Device State

M-Bus devices can be in one of three states:

- Installation mode: In installation mode wireless M-Bus devices will broadcast requests so that an E-meter can register it.
- Customer mode: after a wireless M-Bus device receives its CNF_IR, it will start normal operation in Customer mode as described elsewhere in this document.
- Service mode: a vendor specific mode; not in the scope of this document.

9.3Wireless device address

Wireless M-Bus devices must have a unique device address in the range of the M-Bus transmission. The definition of the address is provided in section 4.2.2 When the M-Bus device is installation mode, it will start periodic transmissions of installation messages (SND_IR) with the Short ID as sender address, see section 4.4.6 The selected E-meter shall respond with a confirmation message (CNF_IR) to the specific M-Bus device.

9.4M-Bus Device Binding

The E-meter needs to bind the M-Bus device to the DLMS/COSEM objects. Interaction between the back office (central system) and the E-meter is through the DLMS protocol. In the following, the interaction of the application in the E-meter and the various protocols is described, followed by an installation procedure (M-Bus binding procedure; there may be more scenario's possible).

The different scenario's and operation of the devices by the installer is described in detail in the document 'Uniform binding process [6]', which describes the following scenario's:

- Binding process with one M-Bus device
- Re-binding process with one M-Bus device already bound
- Binding process with multiple M-Bus devices
- Binding process when power outage occurs

For the purpose of describing the protocol only the Local M-Bus binding procedure is described in this document, see par 9.6.

9.5E-Meter interaction

1) The E-meter always sends a CNF_IR to a *registered* M-Bus device, after reception of a SND_IR of that *registered* M-Bus device. No further action follows, the E-meter just responds with the appropriate message;
2) An M-Bus device is called *registered* in the E-meter when the Short ID (see section 4.2.2) values are written in respective DLMS/COSEM M-Bus objects;
3) An M-Bus device is registered in the E-meter through:
    a. Manual selection from a display at the E-meter of a (unregistered) M-Bus device that sends an SND_IR message. The E-meter shall be in Installation mode to display the received serial number. The E-meter will load the M-Bus Short ID found in the SND_IR message after manual selection;
    b. Writing M-Bus device Short ID in the M-Bus Client object, through the P3 port by the CS.

9.6Local M-Bus Binding Procedure

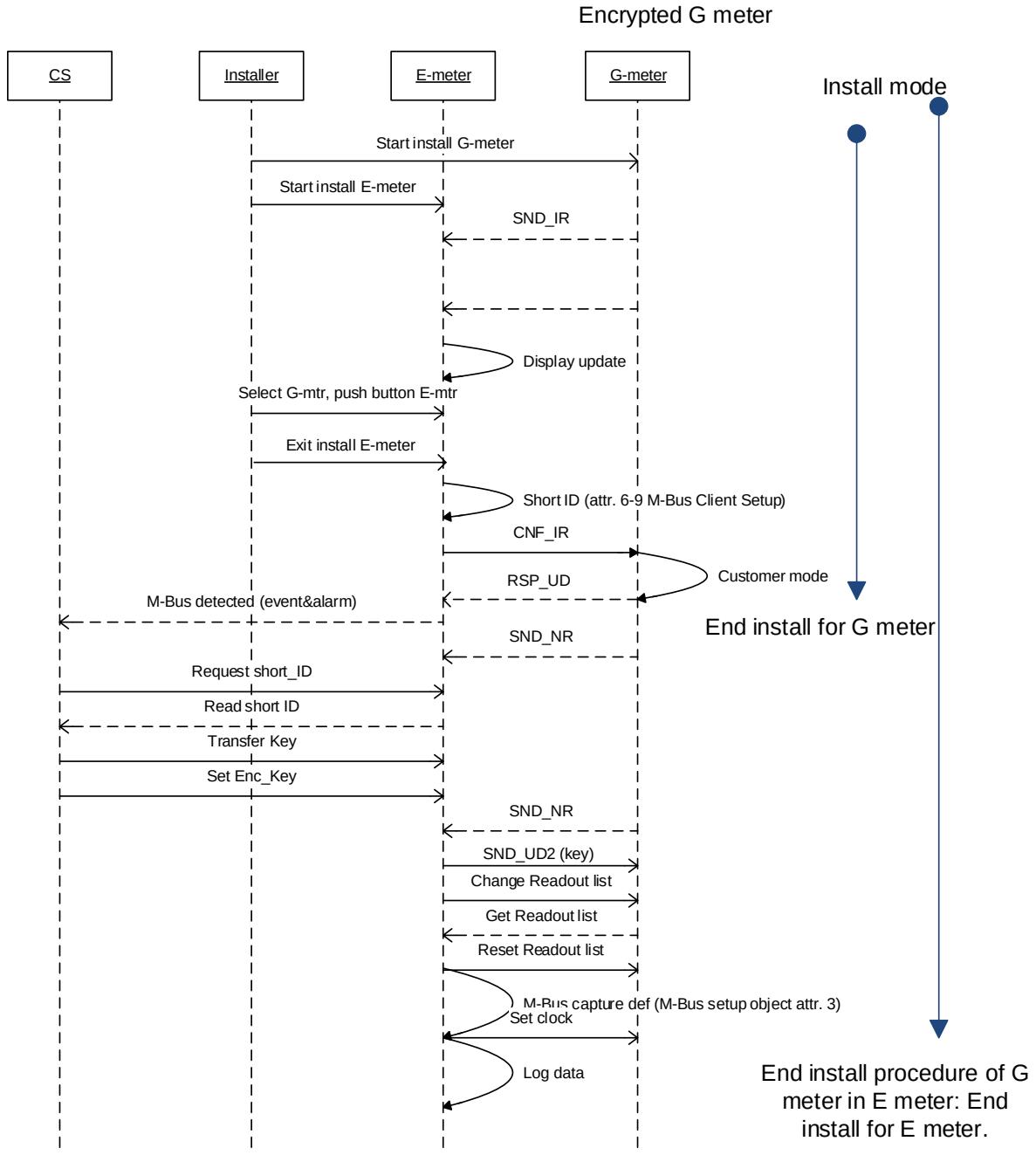


Figure 15: Example wireless binding procedure with manual selection.

Figure 15 describes how an installer manually starts the M-bus installation process by starting the install mode on the G-meter and by starting the install mode on the E-meter.

The various steps are in detail:

1. The installer instructs the M-Bus device to go into Installation mode;
2. The installer instructs the E-meter to go into Installation mode.
3. The M-Bus device sends a SND_IR containing the Short ID as sender address (ref.4.2.1);
4. The M-Bus device sends out SND_IR messages every minute for a period of 30 minutes. If the M-Bus device hasn't received a CNF_IR after 30 minutes yet then the M-Bus device will continue sending SND_IR messages every hour. It must be possible to return to sending SND_IR every minute again for half an hour by means of the push-button;
5. The correct M-Bus device is selected by the E-meter acc to the 'Uniform binding process [6]'. The E-meter writes the Short ID from the SND_IR message of the selected M-Bus device into the DLMS objects;
6. Once the Short ID of the M-Bus device is written in the E-meter's DLMS objects and the E-meter receives a SND_IR message of that M-Bus device, the E-meter replies with a CNF_IR;
7. After receiving the CNF_IR the M-Bus device replies with an immediate RSP_UD (daily (long) hourly message, including the equipment identifier); the E-meter can optionally open a FAC; The equipment identifier is directly available on the P1 port of the E-meter.
8. The E-meter now prompts 'bound'; the installer exits install mode on the E-meter;
9. The G-meter shows the serial number of the E-meter to which it is bound, on its display
10. From this moment on the M-Bus device will send regular hourly and 5 minutes data, by sending hourly SND_NR messages and 5-min C1-mode messages including meter reading. Notice that the keys of the M-Bus device are not yet set and unknown by the E-meter. As the clock is not set yet, the time of the first hourly transmission of the M-Bus device appears as completely random for the E-meter;
11. Upon receiving a set of keys from the CS, the E-meter shall send the encrypted key to the M-Bus device as described in section 6.5.1. There is no timing restriction on the exchange of User keys;
12. After the keys are set in both the E-meter and the M-Bus device, also the clock of the M-Bus device can be set[5];
13. The E-meter shall retrieve detailed version info from the M-Bus device by modifying the standard readout list.

[5] Because the M-bus device is delivered unencrypted the time can also be set directly after the first SND-NR message without setting the keys first.

After these steps the M-Bus device will send regular hourly and 5 minutes data, by sending SND_NR messages including meter reading data. Now the keys and the clock of the M-Bus device are set and synchronised with the E-meter.

10BACKWARDS COMPATIBILITY

There is no backwards compatibility with earlier DSMRx.x products.

11INTERFERENCE BETWEEN WIRELES M-BUS AND LTE

Situation:

- For communication between E- and G-meters (P2 communication) Wireless M-Bus T2/C mode (868 MHz), is used since the beginning of the DSMR projects and also in the ESMR.
- For communication between the Central System (P3 communication) and the E-meters LTE (4G) will be used in the next generation of meters.

Complication:

- LTE uses nearly the same frequency (band 20). The uplink is from 852-862 MHz (from meter to base station) and the downlink (from base station to meter) from 811-821 MHz.
- LTE uses also other frequency bands but especially band 20 is used for coverage and is the most important one.
- It is certain that interference will occur, the probability and the impact depends on a number of variables.
- LTE is robust (has implemented retry mechanisms), but wireless M-Bus isn't.

With the help from a third party, we made a theoretical analysis of this interference, including simulations. Outcome of this simulations can be found in two reports [9], [10] and are summarised in an overall power-point with the conclusions [11].

Requirement:

Enexis expects at least 99,5% availability of Gas meter readings (5 min and hourly values) for each individual meter.

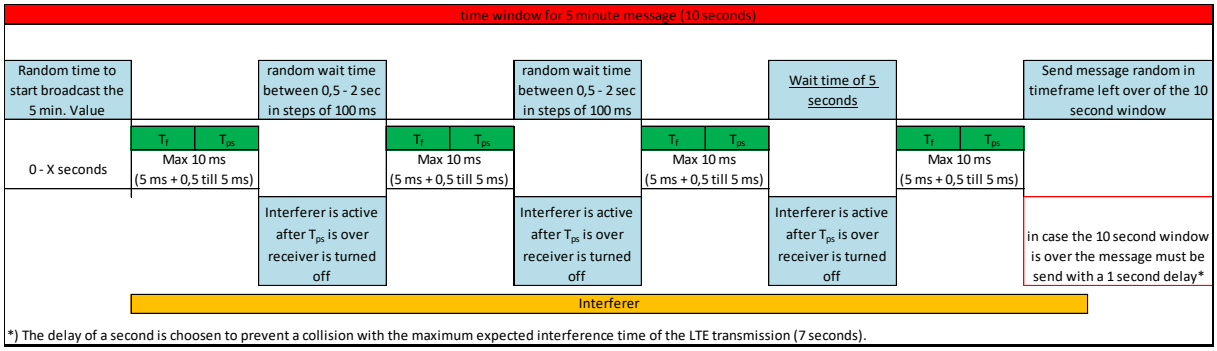
Remark:
The sending of the 3 previous hourly values each hour, may not be used to reach this availability of 99,5% (for 5 min values this is even physically not possible because only one value is send each interval).

11.1CSMA mechanism

CSMA mechanism must be implemented on wM-Bus devices.

Parameters for the CSMA mechanism should be:

- The total listen time, t_L consists of a fixed part, t_F and a pseudo random part, t_{PS}:
  $t_L = t_F + t_{PS}$
  a) The fixed part of the minimum listening time, t_F shall be 5 ms.
  b) The pseudo random listening time t_{PS} shall be randomly varied between 0 ms and 5 ms or more in equal steps of approximately 0,5 ms as the following:
  - If the channel is free from traffic at the beginning of the listen time t_L and remains free throughout the fixed part of the listen time, t_F then the pseudo random part t_{PS} is automatically set to zero by the equipment itself.
  - If the channel is occupied by traffic when the equipment either starts to listen or during the listen period, then the listen time commences from the instant that the intended channel is free. In this situation the total listen time t_L shall comprise t_F and the pseudo random part, t_{PS}.
  The limit for total listen time for the receiver consists of the sum of a) and b) together.
- The channel occupation power level limit: -85 dBm (for 200 kHz receiver BW), referred to an antenna gain of +2 dBi. In case of a different antenna gain (g), the detection limit (P_LBT,DetThr) needs to be adjusted according to the appropriate antenna gain: P_LBT,DetThr=-85 dBm - 2 dBi + g.
- The maximum number of retries must be set to 3. The messages must be transmitted latest with the 3rd retry (4th try) and must be send always (even if it is outside the randomization window of 10 minutes for an hourly value and 10 seconds for a 5 minute value). In case a retry mechanism is needed, the procedure to follow is described in the figure below.



In addition:

- The measurement bandwidth for the channel power must be in regions of the desired bandwidth to be transmitted (200 kHz +/-20%).
- The maximum sample interval for the power detection within the listening time must be 1 ms, i.e. within a period of 5 ms, there must be a min. of 5 channel power level samples available. The maximum detected power level of these samples shall be below the defined threshold.
- For hourly messages the implementation of the algorithm is the same as for the 5 minute message. The only difference is the time window which is 9 minutes instead of 10 seconds. The only difference is that you have a bigger time window left over at the end if you need all the retries. Here is stated that the message will be send randomly in the left over time frame if possible.
- For push messages the implementation of the algorithm is the same as for the 5 minute message. The only difference here is that there is no randomized start. If all retries are needed then after the last retry wait for 1 second and send the message.

11.2Blocking filters

For both wM-Bus devices and E-meters, blocking filters (as defined in ETSI EN300 220 class 1 receiver: but with a value of more than ~60 dB for +/- 2 MHz and +/- 10 MHz offset) are required, to provide the minimum required blocking in the desired receive modes.

APPENDIX A: P2 – P3 MAPPING

DIF	DIF E	VIF	VIFE	Value	Section	P3 reference	
				M-Bus Client Setup object	**4.2.3**	**0-x.24.1.0.255-** (version)	
0Dh		78h		Equipment identifier	**6.4.1**	P3 section 7.2 **0-x:96.1.0.255** (x=channel number (1..4))	Set by manufacturer, read-only. This is a 17 byte field.
4Ch		13h		Gas meter reading, converted 5 min. value (G4 and G6)	**6.4.4.2**	**0-x:24.2.1.255** (x=channel number (1..4))	No storage in load profile, only presented at P1 port directly
4Ch		13h		Gas meter reading, converted hourly value (G4 and G6)	**6.4.4.1**	**0-x:24.3.0.255** Hourly load profile values (x=channel number (1-4)) Capture Objects **0-x:99.2.0.255** Daily load profile values (x=channel number (1-4)) Capture Objects **0-x:98.1.0.255** Monthly Billing values (x=channel number (1-4)) Capture Objects	0-x:24.2.3.255 is used as M-Bus Master value within the load profile
4Ch		14h		Gas meter reading, converted 5 min. value (G10-G25)	**6.4.4.2**	**0-x:24.2.1.255** (x=channel number (1..4)) Capture_Objects	No storage in load profile, only presented at P1 port directly
4Ch		14h		Gas meter reading, converted hourly value (G10-G25)	**6.4.4.1**	**0-x:24.3.0.255** Hourly load profile values (x=channel number (1-4)) Capture Objects	0-x:24.2.3.255 is used as M-Bus Master value within the load profile
4Ch		0Fh		Thermal (Heat) Meter Reading 5 min. value in GJ	**6.4.5**	**0-x:24.2.1.255** (x=channel number (1..4)) Capture_Objects	No storage in load profile, only presented at P1 port directly
4Ch		0Fh		Thermal (Heat) Meter Reading hourly value in GJ	**6.4.5**	**0-x:24.3.0.255** Hourly load profile values (x=channel number (1-4)) Capture Objects **0-x:99.2.0.255** Daily load profile values (x=channel number (1-4)) Capture Objects **0-x:98.1.0.255** Monthly Billing values (x=channel number (1-4)) Capture Objects	0-x:24.2.3.255 is used as M-Bus Master value within the load profile
4Ch	40h	0Fh		Thermal (Cold) meter reading 5 min. value in GJ	**6.4.5**	**0-x:24.2.1.255** (x=channel number (1..4)) Capture_Objects	No storage in load profile, only presented at P1 port directly
4Ch	40h	0Fh		Thermal (Cold) meter reading hourly value in GJ	**6.4.5**	**0-x:24.3.0.255** Hourly load profile values (x=channel number (1-4)) Capture Objects **0-x:99.2.0.255** Daily load profile values (x=channel number (1-4)) Capture Objects **0-x:98.1.0.255** Monthly Billing values (x=channel number (1-4)) Capture Objects	0-x:24.2.3.255 is used as M-Bus Master value within the load profile

4Ch		13h		Thermal (Heat) meter reading Volume 5 min. value in m^3	**6.4.5**	**To be specified**	No storage in load profile, only presented at P1 port directly
4Ch		13h		Thermal (Heat) meter reading Volume hourly value in m^3	**6.4.5**	**To be specified**	0-x:24.2.3.255 is used as M-Bus Master value within the load profile
4Ah		5Ah		Thermal (Heat/Cold) meter forward temperature	**6.4.5**	**To be specified**	
4Ah		5Eh		Thermal (Heat/Cold) meter return temperature	**6.4.5**	**To be specified**	
4Ch		13h		Water meter reading 5 min. value in m^3	**6.4.6**	**0-x:24.2.1.255** (x=channel number (1..4)) Capture_Objects	No storage in load profile, only presented at P1 port directly
4Ch		13h		Water meter reading hourly value in m^3	**6.4.6**	**0-x:24.3.0.255** Hourly load profile values (x=channel number (1-4)) Capture Objects **0-x:99.2.0.255** Daily load profile values (x=channel number (1-4)) Capture Objects **0-x:98.1.0.255** Monthly Billing values (x=channel number (1-4)) Capture Objects	0-x:24.2.3.255 is used as M-Bus Master value within the load profile
4Ch		03h		Slave E-meter reading 5 min. value in Wh	**6.4.7**	**0-x:24.2.1.255** (x=channel number (1..4)) Capture_Objects	No storage in load profile, only presented at P1 port directly
4Ch		03h		Slave E-meter reading hourly value in Wh	**6.4.7**	**0-x:24.3.0.255** Hourly load profile values (x=channel number (1-4)) Capture Objects **0-x:99.2.0.255** Daily load profile values (x=channel number (1-4)) Capture Objects **0-x:98.1.0.255** Monthly Billing values (x=channel number (1-4)) Capture Objects	0-x:24.2.3.255 is used as M-Bus Master value within the load profile
0Dh		FDh	19h	Encrypted user key	**6.5.1**		
04h		FDh	17h	Status Word	**6.3.3**	Directly mapped to events (P3 Companion Standard)	

Header Data (ref 4.2.2.)

M-Bus Field name	P3 reference
Ident Number	**0-x:24.1.0.255** – identification_number
Manufacturing ID	**0-x:24.1.0.255** – manufacturer_id
Version	**0-x:24.1.0.255** – version: fixed 50h
Medium	**0-x:24.1.0.255** – device_type
Access Number	**0-x:24.1.0.255** – access_number
Status – alarm flags	**Used for RSSI**
Configuration – Encryption method	None

Alignment with DLMS Blue Book image transfer:

Step	DLMS Mechanism	M-Bus mapping
1	Get Image Block Size	Firmware upgrade start
2	Initiate Image transfer	Firmware upgrade start
3	Transfer Image Blocks	Firmware upgrade send data
4	Check completeness of the Image	Firmware upgrade request block status
5	Verify Image	Firmware upgrade verify
6	Check the Image before activation	None – internal step
7	Activate Image	Firmware upgrade activate
8	None	Firmware upgrade cancel

APPENDIX B: MESSAGE EXAMPLES

All examples in this document use the following values:

- Equipment Identifier is 'XXXXX0123456789YY'
- Identification Number is '23456789'
- Manufacturer Identification is 'NET' (hex): 38 B4
- Version Identification is the ESMR 5.0 (50h)
- Device Type identification is gas (03h)
- Default Key (hex): 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
- User Key (hex): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
- Frame Counter (hex): 00 00 00 01
- Examples with encryption method = 0x09

Remark in general:
Only hourly messages use the Extended Link Layer (for signaling the availability of the FAC).
Messages from "Other" to "Meter" (E-meter to G-meter) don't use the ELL.

B1.1 Example Key change

The User Key is encrypted with the Default Key: 27 9F B7 4A 75 72 13 5E 8F 9B 8E F6 D1 EE E0 03

Field	Hex	Remark
Length	53h	Length of message
C-Field	43h	SND_UD2
M-Field	M-0	E-Meter MF ID
	M-1	
A-Field	A-0	E-Meter short ID
	A-1	
	A-2	
	A-3	
	50h	Version: ESMR 5.0
	02h	Device Type: Electricity
CRC	XX	
	YY	
CI-Field	5Bh	ESMR master to slave long header
Identification Number	89h	23456789
	67h	
	45h	

Field	Hex	Remark
	23h	
Manufacturer ID	B4h	NET
	38h	
Version	50h	ESMR 5.0
Device type	03h	Gas meter
Access No	AC-0	Access Number
Status	ST-0	RSSI value
Configuration Word	00h	no encryption
	00h	
VIFE	19h	Security key
LVAR	1Ch	4 Byte KCC + 16 Byte User Key + 8 Byte tag
Key change counter	00h	32-bit integer counter value = 00 00 00 01 (MSB first)
CRC	XX	
	YY	
	00h	
	00h	
	01h	
Encrypted key data	KI-0	Key ID
	KS-0	Key Size
	27h	User Key 1 (MSB)
	9Fh	User Key 2
	B7h	User Key 3
	4Ah	User Key 4
	75h	User Key 5
	72h	User Key 6
	13h	User Key 7
	5Eh	User Key 8
	8Fh	User Key 9
	9Bh	User Key 10
	8Eh	User Key 11
CRC	XX	
	YY	
	F6h	User Key 12
	D1h	User Key 13
	EEh	User Key 14
	E0h	User Key 15
	03h	User Key 16 (LSB)
GCM authentication tag	AT-0	GCM authentication tag where AT0 is the MSB of the GMAC
	AT-1	
	AT-2	

Field	Hex	Remark
	AT-3	
	AT-4	
	AT-5	
	AT-6	
	AT-7	
CRC	XX	
	YY	

B1.2 Example Retrieve version information

1. Selecting the data to retrieve (Hardware and Metrology version)

Request		
Field	**Hex**	**Remark**
Length	2Eh	Length of message
C-Field	43h	SND_UD2
M-Field	M-0	E-Meter MF ID
	M-1	
A-Field	A-0	E-Meter short ID
	A-1	
	A-2	
	A-3	
	50h	Version: ESMR 5.0
	02h	Device Type: Electricity
CRC	XX	
	YY	
CI	5Bh	ESMR master to slave long header
Identification Number	89h	23456789
	67h	
	45h	
	23h	
Manufacturer ID	B4h	NET
	38h	
Version	50h	ESMR 5.0
Device type	03h	Gas meter
Access No	AC-0	Access Number
Status	ST-0	RSSI value
Configuration Word	01h	User Key1
	29h	Security Mode 9, Tag present
Length [E]	06h	6 encrypted APL bytes

Length [U]	00h		no unencrypted bytes
Message Counter	00h		00 00 00 01
CRC	XX		
	YY		
	00h		
	00h		
	01h		
DIF	08h	enc	Request for readout (Hardware version #)
VIF	FDh	enc	
VIFE	0Dh	enc	
DIF	08h	enc	Request for readout (Metrology (firmware) version #)
VIF	FDh	enc	
VIFE	0Eh	enc	
GCM authentication tag	AT-0		
	AT-1		
	AT-2		
	AT-3		
	AT-4		
	AT-5		
	AT-6		
CRC	XX		
	YY		
	AT-7		
	AT-8		
	AT-9		
	AT-10		
	AT-11		
CRC	XX		
	YY		

2. Requesting the data

Response			
Field	**Hex**		**Remark**
Length	55h		Length of message
C-Field	08h		Sending of the required data (RSP_UD)
M-Field	B4h		NET
	38h		
A-Field	89h		23456789
	67h		
	45h		
	23h		
	50h		Version: ESMR 5.0
	03h		Device Type: Gas meter
CRC	XX		
	YY		
CI-Field	8Ch		Extended Link Layer
CC-Field	80h		limited access
ACC-Field	AAh		ELL-Access Counter of Meter
CI-Field	7Ah		Slave to Master short header
Access No	AAh		Access Number = ELL ACC Field
Status	ST-0		RSSI value
Configuration Word	01h		User Key1
	29h		Security Mode 9, Tag present
Length [E]	32h		50 encrypted APL bytes
Length [U]	00h		no unencrypted bytes
Message Counter	00h		00 00 00 01
	00h		
	00h		
	01h		
DIF	0Dh	enc	Variable length string
VIF	FDh	enc	Hardware version number
CRC	XX		
	YY		
VIFE	DCh	enc	
LVAR	1Bh	enc	Length = 27
8 bit string (LSB first)	0Ah	enc	LF
	0Dh	enc	CR
	72h	enc	r
	65h	enc	e
	69h	enc	i
	6Ch	enc	l
	70h	enc	p

	70h	enc	p
	75h	enc	u
	73h	enc	s
	20h	enc	
	65h	enc	e
	6Ch	enc	l
	75h	enc	u
CRC	XX		
	YY		
	64h	enc	d
	6Fh	enc	o
	6Dh	enc	m
	20h	enc	
	73h	enc	s
	75h	enc	u
	62h	enc	b
	2Dh	enc	-
	4Dh	enc	M
	3Dh	enc	=
	6Dh	enc	m
	6Fh	enc	o
	63h	enc	c
DIF	0Dh	enc	Variable length string
VIF	FDh	enc	Metrology (firmware) version number
VIFE	0Ch	enc	
CRC	XX		
	YY		
LVAR	0Fh	enc	Length = 15
8 bit string (LSB first)	0Ah	enc	LF
	0Dh	enc	CR
	35h	enc	5
	2Eh	enc	.
	34h	enc	4
	2Eh	enc	.
	33h	enc	3
	32h	enc	2
	31h	enc	1
	57h	enc	W
	46h	enc	F
	3Dh	enc	=
	74h	enc	t
	65h	enc	e

	6Dh	enc	m
CRC	XX		
	YY		
GCM authentication tag	AT-0		
	AT-1		
	AT-2		
	AT-3		
	AT-4		
	AT-5		
	AT-6		
	AT-7		
	AT-8		
	AT-9		
	AT-10		
	AT-11		
CRC	XX		
	YY		

3. Resetting the request list

Request		
Length	28h	Length of message
C-Field	40h	SND_NKE
M-Field	M-0	E-Meter MF ID
	M-1	
A-Field	A-0	E-Meter short ID
	A-1	
	A-2	
	A-3	
	50h	Version: ESMR 5.0
	02h	Device Type: Electricity
CRC	XX	
	YY	
CI-Field	80h	Long header no payload
Identification Number	89h	23456789
	67h	
	45h	
	23h	
Manufacturer ID	B4h	NET
	38h	
Version	50h	ESMR 5.0
Device type	03h	Gas meter
Access No	AC-0	Access Number
Status	ST-0	RSSI value
Configuration Word	01h	User Key1

	29h	Security Mode 9, Tag present
Length [E]	00h	no encrypted bytes
Length [U]	00h	no unencrypted bytes
Message Counter	00h	00 00 00 01
CRC	XX	
	YY	
	00h	
	00h	
	01h	
GCM authentication tag	tag-0	
	tag-1	
	tag-2	
	tag-3	
	tag-4	
	tag-5	
	tag-6	
	tag-7	
	tag-8	
	tag-9	
	tag-10	
	tag-11	
CRC	XX	
	YY	

B1.3 RSP_UD telegram of a Gas Meter

This example shows a RSP_UD telegram (before encryption) of a meter comprising of the following properties:

- temperature converted volume
- meter type G4 => volume multiplier = 0,001m³

Field	Hex		Remark
	clear	encrypted	
Length	43h		Length of message
C-Field	08h		RSP_UD
M-Field	B4h		
	38h		'NET'
A-Field	89h		
	67h		
	45h		
	23h		ID: '23456789'
	50h		Version: ESMR 5.0
	03h		Device Type: Gas meter
CRC	XX		
	YY		
CI-Field	8Ch		Extended Link Layer
CC-Field	80h		limited access
ACC-Field	AAh		ELL-Access Counter of Meter
CI-Field	7Ah		Slave to Master short header
Access No	AAh		Access Number = ELL ACC Field
Status	ST-0		RSSI value
Configuration Word	01h		User Key1
	29h		Security Mode 9, Tag present
Length [E]	2Ah		42 encrypted APL bytes
Length [U]	00h		no unencrypted bytes
Message Counter	00h		00 00 00 01
	00h		
	00h		
	01h		
DIF	01h	enc	8 bits
VIF	FDh	enc	Use VIFE
CRC	XX		
	YY		
VIFE	17h	enc	Error flags
Status byte	00h	enc	Encrypted Status
DIF	0Dh	enc	variable length
VIF	78h	enc	Serial number
LVAR	11h	enc	Serial number length 17 Field

Field	Hex		Remark
	clear	encrypted	
Equipment Identifier	39h	enc	’XXXXX110123456789’
	38h	enc	
	37h	enc	
	36h	enc	
	35h	enc	
	34h	enc	
	33h	enc	
	32h	enc	
	31h	enc	
	30h	enc	
	31h	enc	
CRC	XX		
	YY		
Equipment Identifier (continue)	31h	enc	
	58h	enc	
	58h	enc	
	58h	enc	
	58h	enc	
	58h	enc	
DIF	46h	enc	6 bytes integer, storage bit set
VIF	6Dh	enc	Date and Time data type I
	00h	enc	
	00h	enc	
	0Bh	enc	
	32h	enc	
	16h	enc	Date/Time (yy.mm.dd
Time stamp	00h	enc	hh:mm:ss) = 09.06.18 11:00:00
DIF	4Ch	enc	8 digit BCD storage 1
VIF	13h	enc	Volume (0,001 m³)
CRC	XX		
	YY		
	91h	enc	
Meter value	03h	enc	
(converted volume)	00h	enc	’00000391’
Meter value	00h	enc	
DIF	01h	enc	1 digit binary
VIF	FDh	enc	Extension
VIFE	67h	enc	Special Supplier Information
GCM authentication tag	AT-0		
	AT-1		

Field	Hex		Remark
	clear	encrypted	
	AT-2		
	AT-3		
	AT-4		
	AT-5		
	AT-6		
	AT-7		
CRC	XX		
	YY		
	AT-8		
	AT-9		
	AT-10		
	AT-11		
CRC	XX		
	YY		

B1.4 Example C1 telegram of a Gas Meter

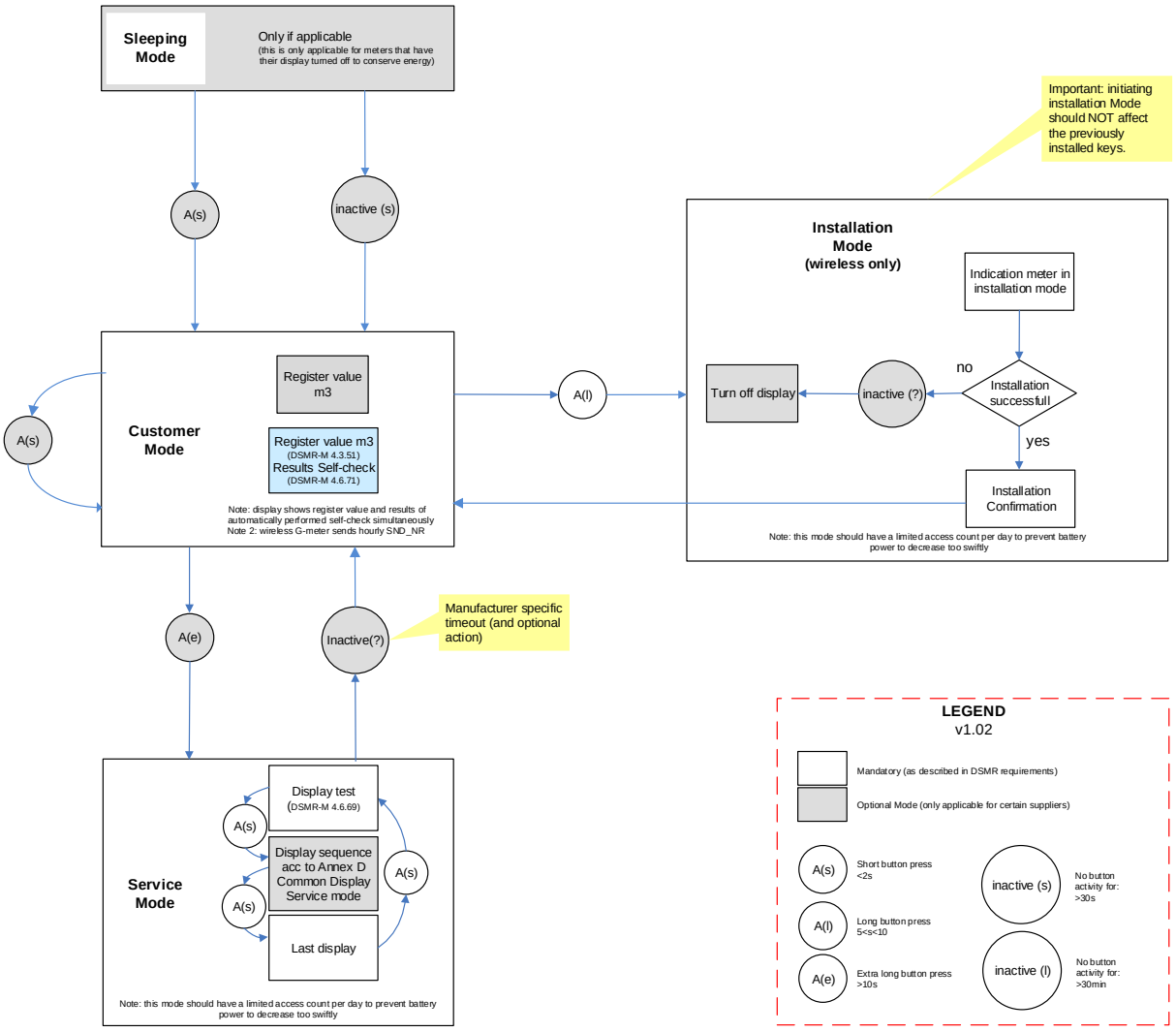
This example shows a mode C1 telegram that is used to send the 5 minute interval real time value. It contains both a timestamp and a volume.

- Identification Number is '23456789'
- Manufacturer Identification is 'NET' (hex): 38 B4
- Version Identification is the ESMR 5.0 (50h)
- Device Type identification is gas (03h)
- Default Key (hex):00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
- User Key (hex):00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
- Value is 1.234 [m³]
- Timestamp is 2014-04-08 17:05:00

Field	Hex		Remark
	clear	encrypted	
Length	30h		Length of message
C-Field	44h		Send no reply
M-Field	B4h		
	38h		NET
A-Field	89h		
	67h		
	45h		
	23h		23456789
	50h		Version: ESMR 5.0
	03h		Device type: Gas meter
CI-Field	7Ah		Slave to Master short header
Access No	AC-0		Access Number
Status	ST-0		RSSI value
Configuration	01h		User Key1
	29h		Security Mode 9, Tag present
Length [E]	0Eh		14 encrypted APL bytes
Length [U]	00h		no unencrypted bytes
Message Counter	00h		
	00h		
	00h		
	01h		00 00 00 01
DIF	4Ch	enc	Storage 1 digit BCD
VIF	13h	enc	Volume in liter
Value	34h	enc	
	12h	enc	
	00h	enc	
	00h	enc	1.234 [m³]

DIF	46h	enc	Storage 1
VIF	6Dh	enc	Time format I
Value	00h	enc	
	05h	enc	
	11h	enc	
	C8h	enc	
	14h	enc	
	00h	enc	Timestamp: 2014-04-08 17:05:00
GCM authentication tag	AT-0		
	AT-1		
	AT-2		
	AT-3		
	AT-4		
	AT-5		
	AT-6		
	AT-7		
	AT-8		
	AT-9		
	AT-10		
	AT-11		
CRC-field	XX		
	YY		

APPENDIX C: ESMR5 BUTTON PROCESS



APPENDIX D: VENDOR SPECIFIC ERROR BITS

Vendor specific error bits Itron			
Bit	**Meaning with Bit set**	**Significance with Bit not set**	**Push**
20	Powerfail	No Powerfail	no
21	Max Flow	No Max Flow	no
22	TempMinLimit	No TempMinLimit	no
23	TempMaxLImit	No TempMaxLImit	no
24	Pulserror	No Pulserror	no
25	Consumperror	No Consumperror	no
26	reserve	reserve	n/a
27	reserve	reserve	n/a
28	reserve	reserve	n/a
29	reserve	reserve	n/a
30	reserve	reserve	n/a
31	reserve	reserve	n/a

Vendor specific error bits Elster			
Bit	**Meaning with Bit set**	**Significance with Bit not set**	**Push**
20	Tamper Battery	No tamper Battery	yes
21	HLC damage	No HLC damage	yes
22	Permanent Log filled up to 90%	Permanent Log not filled up to 90%	no
23	Device is about to enter hiberna-tion mode	Device is in normal mode	yes
24	Broken case switch detection af-ter OTA-update	No broken case switch detected after OTA-update	no
25	reserve	reserve	n/a
26	reserve	reserve	n/a
27	reserve	reserve	n/a
28	reserve	reserve	n/a
29	reserve	reserve	n/a
30	reserve	reserve	n/a
31	reserve	reserve	n/a

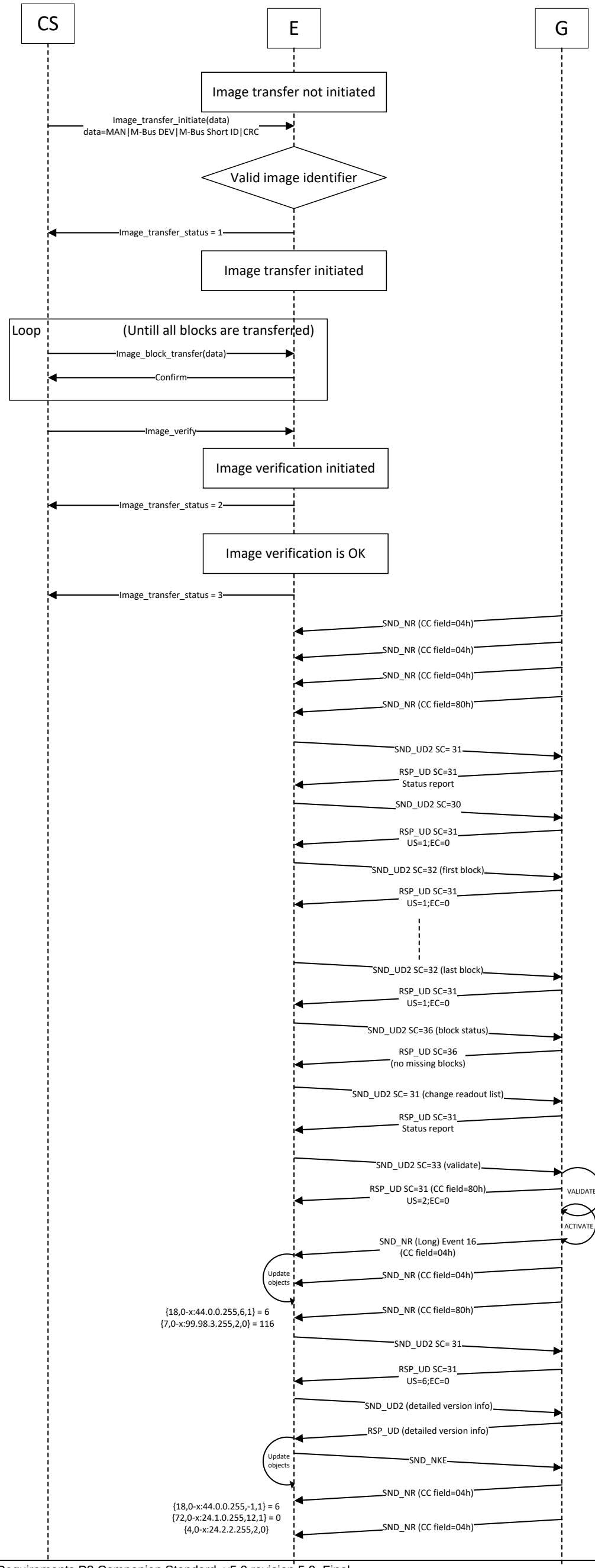
These bits are mapped to events 1xx in P3 Companion Standard (chapter 4.2.1). For example Bit 21 is mapped to event 121.

APPENDIX E: FIRMWARE UPDATE FLOW CHARTS

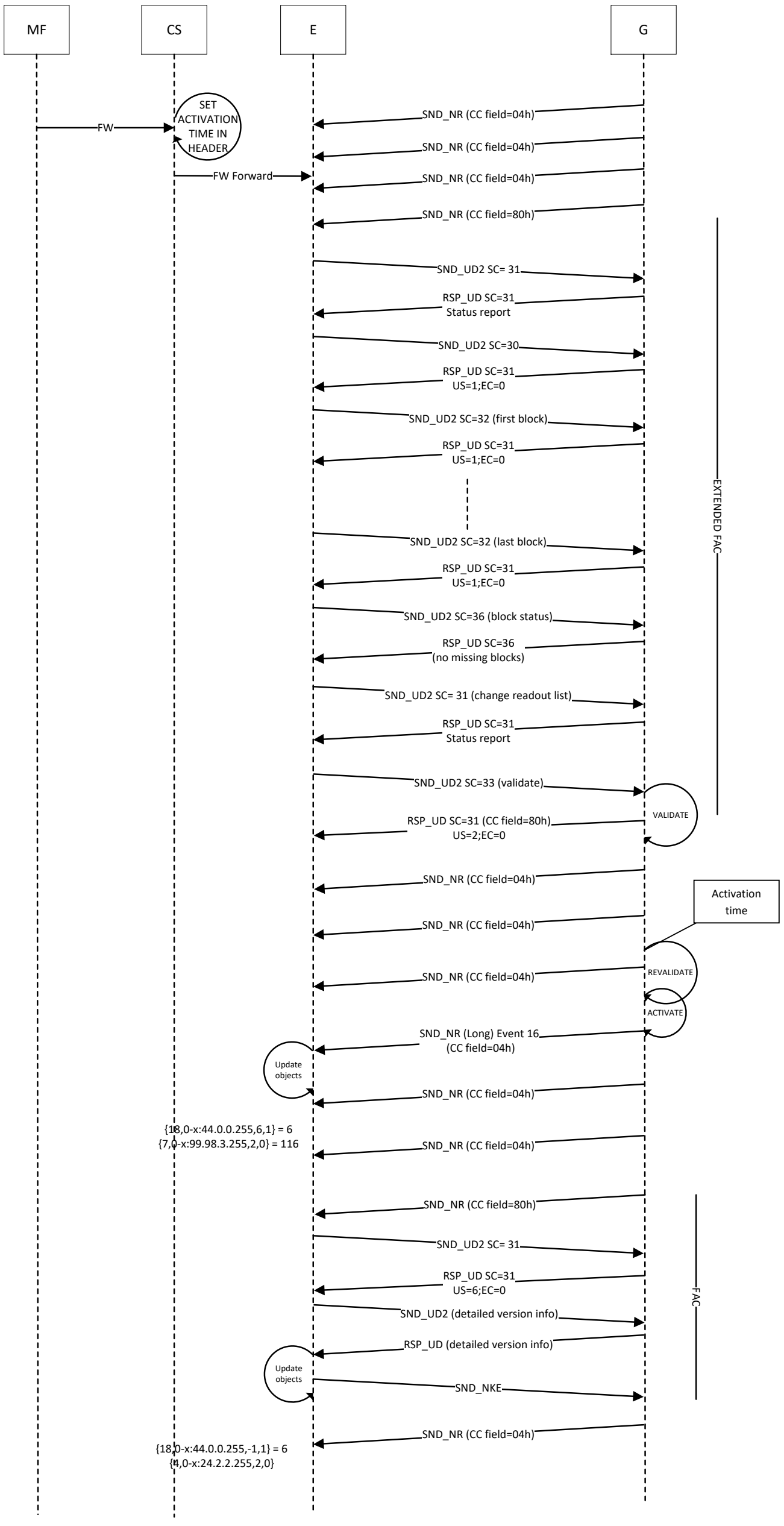
In this appendix the following flow charts are described:

1. CS to M-Bus device Firmware upgrade flow, successful immediate activation
2. CS to M-Bus device Firmware upgrade flow, time based activation
3. CS to M-Bus device Firmware upgrade flow, master initiated activation
4. More than one FAC necessary for the update
5. Missing block(s) during firmware update
6. Corrupt header
7. Authentication not OK

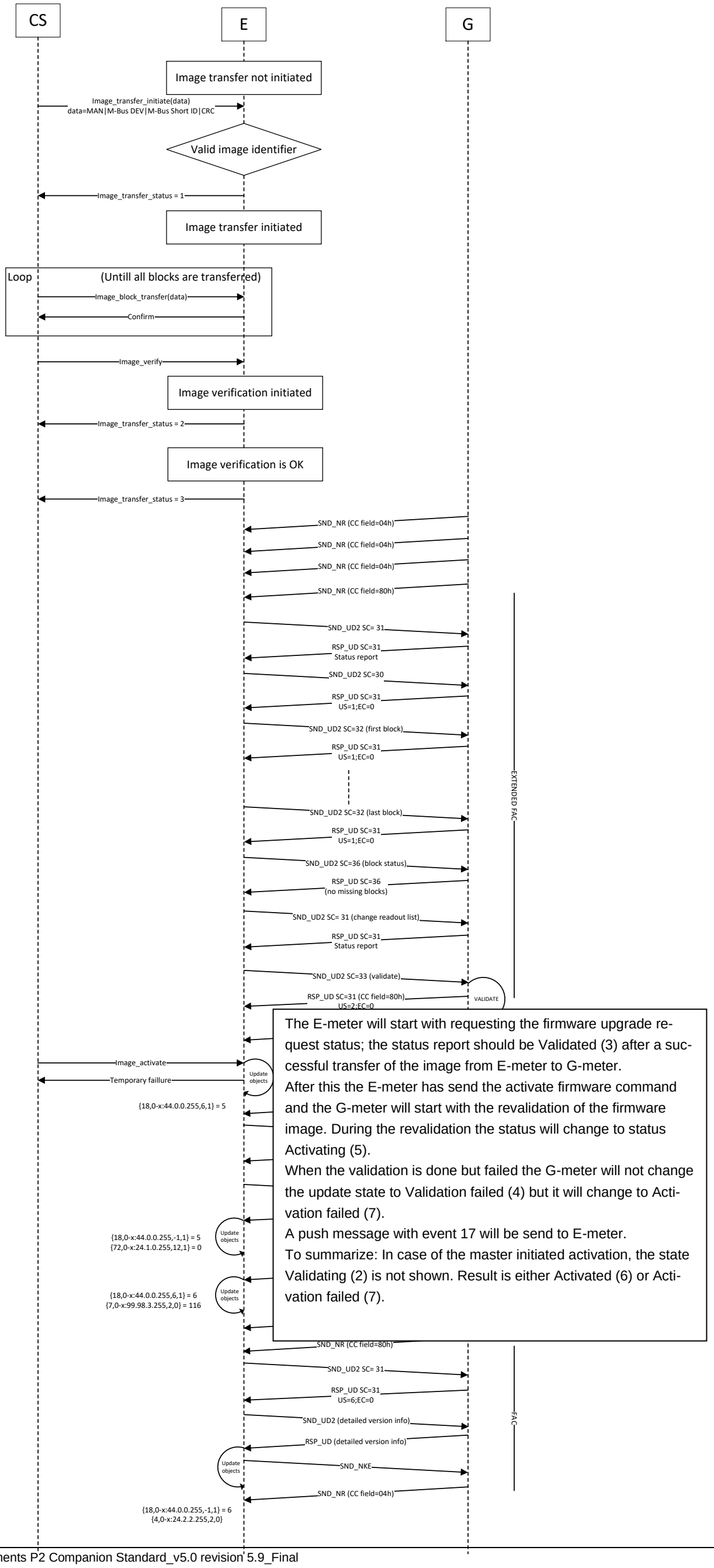
IMMEDIATE ACTIVATION



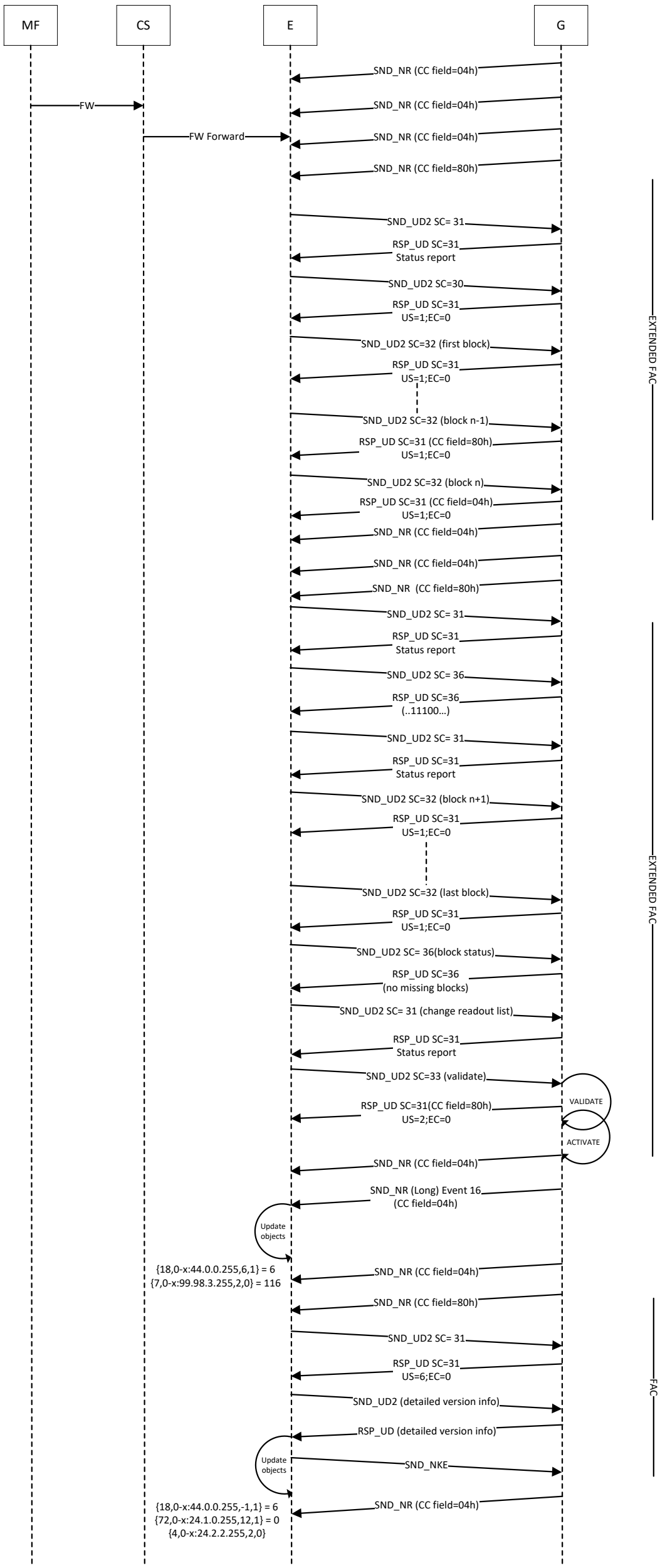
TIME BASED ACTIVATION



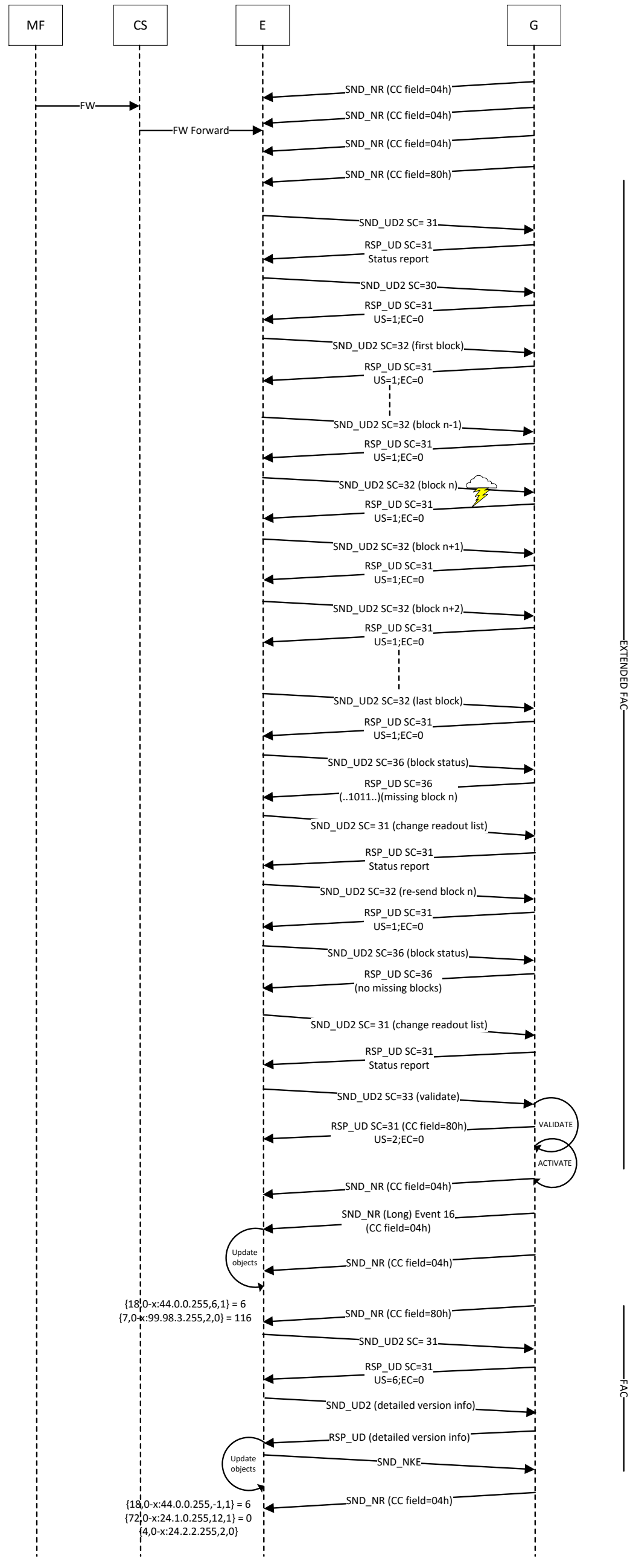
MASTER INITIATED ACTIVATION



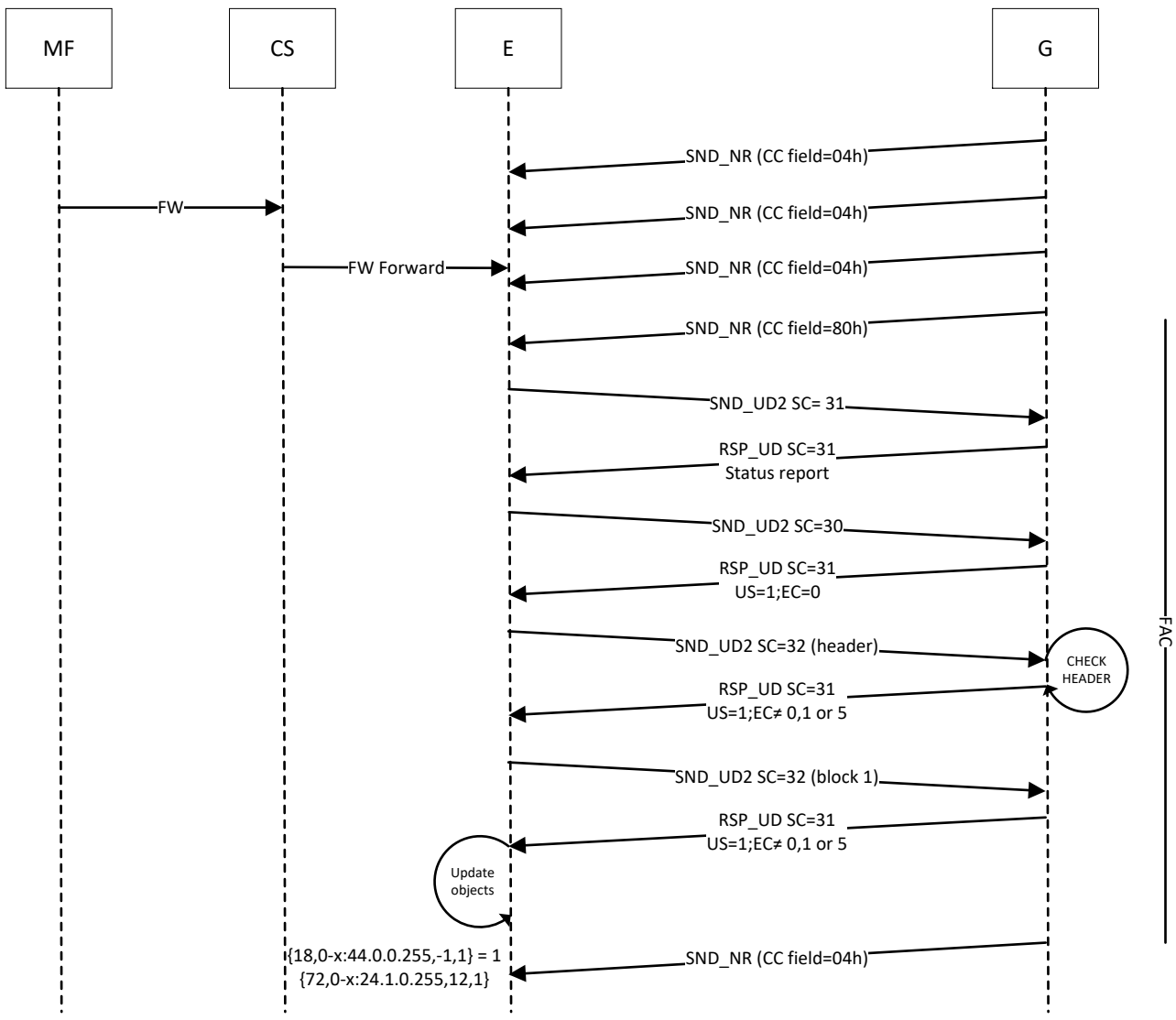
MORE THAN ONE FAC NECESSARY



MISSING BLOCKS



CORRUPT HEADER



AUTHENTICATION NOT OK