IDIS
INTEROPERABILITY SPECIFICATION

Package 2
IP Profile

Edition 2.0 (including G3-PLC), 03-09-2014

Table of Contents

Figures

Tables

1. Foreword

COPYRIGHT

THE USE OF THE IDIS LOGO AND THE IDIS TEST LABEL

The IDIS logo is a registered trademark. The use of the logo is regulated by the IDIS Industry Association.

The IDIS test label is granted by the IDIS Industry Association for registered equipment which has passed the IDIS interoperability test. The interoperability testing and the use of the test label is regulated by the IDIS Industry Association.

2. Scope

2.1 Scope of IDIS

The IDIS Association develops, maintains and promotes publicly available technical interoperability specifications (“IDIS Specifications”) based on open standards and supports their implementation in interoperable products. The Association manages, administers and protects the IDIS quality label (IDIS = “Interoperable Device Interface Specifications”) and supports rigorous interoperability testing to ensure high quality standards.

The IDIS specifications are completely based on existing standards. In order to ensure true interoperability between the IDIS devices the IDIS specifications define specific choices of the different options offered by the standards. The purpose of the IDIS specifications is to close the gaps left by the standards and thus reducing integration and operation costs (comp. Figure 1)

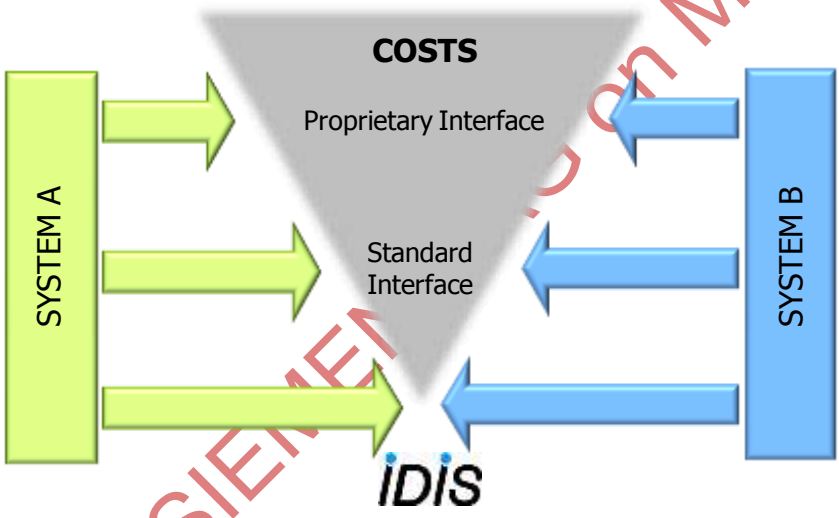


Figure 1: Costs to integrate and operate different types of interfaces

2.2 Scope of this document

This document is part of the IDIS Interoperability Package 2. It specifies the functionality of an IDIS device integrated into a IP communication network.

The functionality of the IDIS device is based on the DLMS/COSEM standards.

3. Introduction

3.1 Referenced Documents

Ref.	Title
DLMS UA 1000-2 Ed. 8.0:2014	*DLMS/COSEM Architecture and Protocols, the "Green Book"*
DLMS UA 1000-1 Ed. 12.0	*COSEM Identification System and Interface Classes, the "Blue Book" Ed. 12*
IDIS P2-OBJ Ed.2.0	*IDIS Package 2, Smart metering Objects, Ed.2.0*
IDIS P1-PLC-P Ed.1.1	*IDIS Package 1, PLC Profile Specification, Ed.1.1*
EN 13757-1:2002	*Communication system for meters and remote reading of meters – Part 1: Data exchange*
EN 13757-2:2002	*Communication system for meters and remote reading of meters – Part 2: Physical and Link layer*
EN 13757-3:2004	*Communication systems for and remote reading of meters – Part 3: Dedicated application layer*
IEC 62056-1-0/Ed.1/FDIS	ELECTRICITY METERING DATA EXCHANGE – The DLMS/COSEM suite – Part 1-0: Smart metering standardisation framewor
IEC 62056-21 Ed. 1.0:2002	*Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange*
IEC 62056-46 Ed. 1.1:2007	*Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol*
IEC 62056-5-3:2013 Amd.1 CDV	ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE – Part 5-3: DLMS/COSEM application layer – Amendment 1
IEC 62056-6-1:2013 Amd.1 CDV	ELECTRICITY METERING DATA EXCHANGE - The DLMS/COSEM SUITE - Part 6-1: Object Identification System (OBIS) – Amendment 1
IEC 62056-6-2:2013 Amd.1 CDV	ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE – Part 6-2: COSEM interface classes – Amendment 1
STD0006 (1980)	User Datagram Protocol. Also: RFC0768
STD0007 (1981)	Transmission Control Protocol. Also: RFC0793
IETF STD 0005:1981	Internet Engineering Task Force (IETF): Internet Protocol. J. Postel. September 1981. (Also IETF RFC0791, RFC0792, RFC0919, RFC0922, RFC0950, RFC1112) Available from: http://www.faqs.org/rfcs/std/std5.html
IETF STD 0051:1994	Internet Engineering Task Force (IETF): The Point-to-Point Protocol (PPP). W. Simpson, Ed.. July 1994. (Also RFC1661, RFC1662) Available from: http://www.faqs.org/rfcs/std/std51.html
"How to get the IDIS Test Label ", R1.1, April 2012"	"How to get the IDIS Test Label ", R1.1, April 2012, IDIS association Available from http://www.idis-association.com
ITU-T G.9903 (05/2013)	SERIES G: TRANSMISSION SYSTEMS AND MEDIA,DIGITAL SYSTEMS AND NETWORKS, Access networks – In premises networks -Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks.
IEEE Std 1901.2-2013	IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communication for Smart Grid Applications

3.2 Terms, Definitions and Abbreviations

Abbreviation	Explanation
AA	Application Association
AARE	Application Association Response

Abbreviation	Explanation
AARQ	Application Association ReQuest
ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
ASE	Application Service Element
A-XDR	Adapted Extended Data Representation
CII	Consumer Information Interface
CIP	Consumer Information Push
class_id	Interface class identification code
COSEM	Companion Specification for Energy Metering
COSEM object	An instance of a COSEM interface class
DC	Data Concentrator used for PLC communication
DLMS	Device Language Message Specification
ERP	Enterprise Resource Planning
FC	Frame Counter
G3	G3 PLC supporting IPv6
GCM	Galois/Counter Mode, an algorithm for authenticated encryption with associated data
UTC	Coordinated Universal Time (replaces GMT in IDIS package 1)
CSD	Circuit Switched Data
HDLC	High-level Data Link Control
HES	Head End System similar to MDC
HLS	COSEM High Level Security
IC	COSEM Interface Class
IEC	International Electrotechnical Commission
LLC	Logical Link Control (Sublayer)
LLS	COSEM Low Level Security
LN	COSEM Logical Name
MDC	Meter Data Collect similar to HES
MDM	Meter Data Management
NN	Neighborhood Network as defined in IEC 62056-1-0/Ed.1/FDISIEC 62056-1-0/Ed.1/FDISIEC 62056-1-0/Ed.1/FDIS
OBIS	Object Identification System
PDU	Protocol Data Unit
PUSH	the data is pushed by the meter to the HES using the Data Notification service
SAP	Service Access Point
SMS	Short Message Service
L_SAP	Link layer Service Access Point

3.2.1 Expressions/Definitions used throughout the document:

Expression	Definition
“reserved” or “reserved for future use”	Strictly reserved for IDIS use; i.e. these values must NOT be used for any manufacturer specific extensions.

“manufacturer specific”	The choice of this parameter is left to the manufacturer: The manufacturer is responsible to avoid any inconsistencies.
“optional “ (features)	These features may be implemented by the manufacturer. The testing of these features is not part of the conformance test.
“optional objects”	The implementation of the “optional objects” is left to the manufacturer. If optional objects are identified in the “Optional Objects List” by the manufacturer they will become part of the conformance test.
“default values”	For conformance testing the manufacturer has to set the attributes to the default values as defined in IDIS P2-OBJ Ed.2.0. For those attributes where no default value is defined the manufacturer may set any value within the allowed range.

3.3 Revision History

Version	Date	Editor	Comment
Edition 1.0		IDIS Association	Internal release
Edition 1.1	30.09.13	IDIS Association	Public release based on w05
Edition 1.2	15.11.13	IDIS Association	Public release based on w09
Edition 2.0	03.09.14	IDIS Association	Public release based on: *draftIDIS-S02-001 E2.0 IDIS Pack2 IP profile 140903* Replaces Ed. 1.2 (15.11.2013) and Corrigendum 2 (02.05.2014).

4. IDIS Conformance Testing

IDIS components are tested for conformity according to the rules set by the IDIS Industry Association. More details can be found in “How to get the IDIS Test Label “, R1.1, April 2012”.

By introducing new mandatory functionalities with a new package N+k a device conforming to package N cannot conform to the specifications of package N+k.

Every IDIS devices carries an **IDIS Test Label** which identifies:

- the *Extensions* (comp. 7.2) to the minimal IDIS functionality implemented in this device
- the *Test Report* produced by the type-testing of this device

Examples of the IDIS test labels:

Device supporting Basic functionality of IDIS package 2

IDIS 2
No 100820

Device supporting Basic, Disconnector and Multi-Utility functionality of IDIS package 2

IDIS 2DM
No 100840

Device supporting Basic, Disconnector. Load Management and Multi-utility functionality of IDIS package 2

IDIS 2DLM
No 100110

The **Test Report** clearly identifies:

- The type and manufacturer of the device
- The Extensions supported by the device
- The additional *Options* supported by the device

Test Reports are available through the IDIS association.

NB: depending on the IP supporting medium, additional medium specific tests may be required by the IDIS association.

5. IDIS System Architecture

5.1 Basic principles

IDIS package 2 supports direct communication between the electricity meter and the HES via interface I3. Further, PLC communication between the meter and the concentrator via interface I3.1 is supported.

The green parts shown in Figure 2 are supported by IDIS package 2.

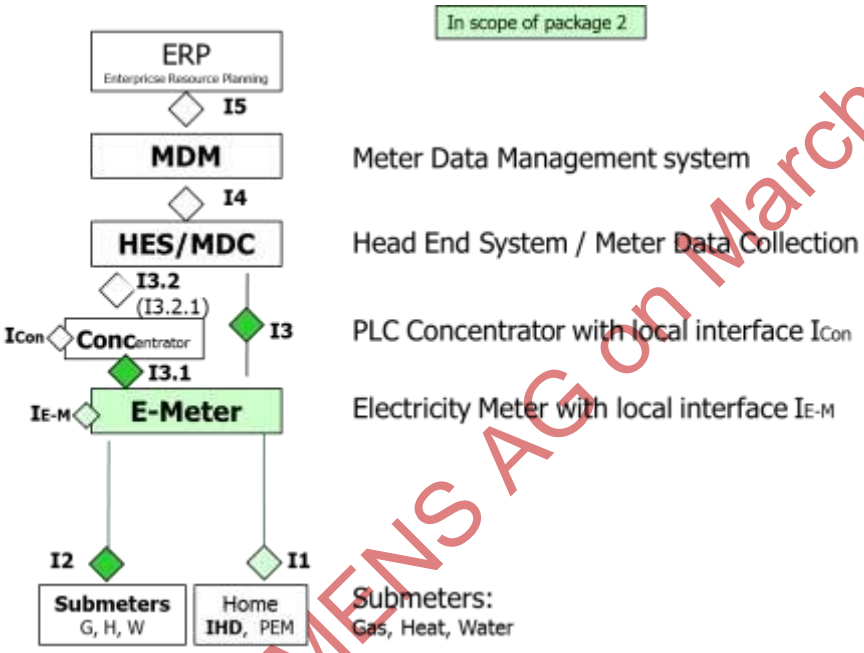


Figure 2: System architecture supported by IDIS package 2

For I1 and I_{E-M} IDIS package 2 defines the required functionality but the choice of the physical interface is left to the manufacturer.

The following interfaces are *NOT* in scope of IDIS package 2: I5, I4, I3.2, and the local interfaces: Icon.

Remark:
The support of interface I3.1 is restricted to PLC technologies based on IPv4/6 communication. IP and the communication layers above are the same for I3.1 and I3. The COSEM client may be located in the HES or in the DC.

5.2 Interface I3

IDIS package 2 supports communication via

- IP networks as specified in DLMS UA 1000-2 Ed. 8.0:2014 and shown in Figure 3.

- SMS service (limited to unconfirmed xDLMS services for PLMN[1] networks)
- CSD / CLIP (limited to wake up calls via PLMN networks)

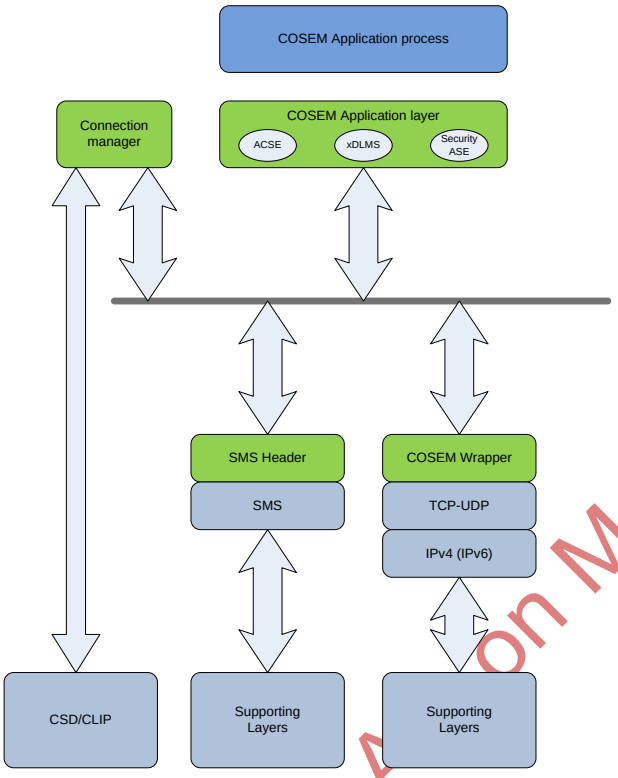


Figure 3: Communication means supported by IDIS package 2

The following "Supporting Layers" are covered by package 2:

- GSM: CSD/CLIP (for wake up only), SMS, GPRS
- 3G
- Ethernet
- G3-PLC

Communication between the HES and the Meter is supported in the following operation modes:

- PULL for 1-way or 2-way communications *initiated by the HES*
- PUSH[2] for 1-way communication *initiated by the Meter*

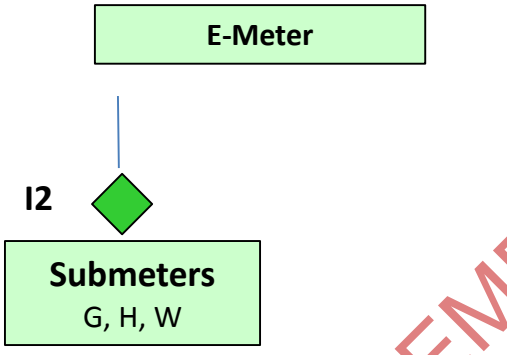
[1] Public Land Mobile Network
[2] Comp. 7.8

Operation mode / usage	DLMS service for IP communication	DLMS services for SMS communication	CSD service
PULL	GET, SET, ACTION	SET (Unconfirmed), ACTION (Unconfirmed)	-
PUSH	DATA-NOTIFICATION (unconfirmed)	DATA-NOTIFICATION (unconfirmed)	-
Wake up	-	-	CLIP caller identification, SMS

Table 1: Operation modes and communication services on different channels

For meters supporting only Ethernet or G3 communication, the wake up service is not supported.

5.3 Interface I2 (submeters)



- The M-Bus is used to connect the submeters (such as Gas, Heat and Water) to the E-Meter.
- The data of the M-Bus devices (according to EN 13757-3) is mapped to COSEM objects in the E-Meter.
- M-Bus devices are always accessed via the COSEM objects in the E-meter (no transparent access through the E-meter)

5.3.1 Wired M-Bus

- The wired M-Bus is based on the EN 13757-2 physical and link layer.
- The format class FT1.2 of EN 60870-5-1 and the telegram structure according to EN 60870-5-2 is used.
- The baud rate is 2400 b/s, E,8,1.

5.3.1.1 Uniqueness of M-bus device identification

According to EN 13757-3 sect. E8.2 the following 4 parameters are needed to guarantee uniqueness of the M-Bus device identification:

- Fabrication Number (DIF/VIF)
- Manufacturer (header of M-Bus frame)
- Version (header of M-Bus frame)
- Medium (header of M-Bus frame)

IDIS provides all information necessary to uniquely identify the device as follows:

M-Bus Information	IDIS object model information
Fabrication Number	Object (IC 1): “M-Bus Device ID 1 channel X” Type octet string containing the ASCII encoded fabrication number. The length of the octet string matches the length of the fabrication number.
Manufacturer	Object (IC 72): M-Bus client channel X Attribute: manufacturer_id
Version	Object (IC 72): M-Bus client channel X Attribute: version
Medium	Object (IC 72): M-Bus client channel X Attribute: device type

For systems where the uniqueness can be guaranteed by the M-Bus “Identification Number” (part of the Data Header of the M-Bus frame according to EN 13757-3:2004, sect. 5.4) IDIS provides this information in the attribute “identification_number” of the object “M-Bus client channel X” (where X=1,2,3, or 4).

M-Bus Information	IDIS object model information
Identification Number 8 BCD digits (part of the Data Header)	Object (IC 72): M-Bus client channel X Attribute: identification_number Type double-long-unsigned. Contains the integer value represented by the 8 BCD digits (not BCD !)

5.3.1.2 Conversion of M-Bus VIF into COSEM scaler_unit

At least one of the following two scenarios must be supported by the E-meter:

1: The e-meter automatically configures the COSEM scaler_unit according to the corresponding information contained in VIF.

2: The COSEM scaler_unit is manually configured in the e-meter (e.g. according to the requirement of the system or display). In this case the e-meter automatically converts the values coming from the M-bus device considering the information provided by VIF. This scenario requires the provision of the optional SET service on attribute scaler_unit of the M-bus value object.

5.3.2 Wireless M-Bus

Wireless M-Bus is not in scope of IDIS package 2.

6. Use Cases supported by IDIS package 2

The following Use Cases (comp. Table 2) are supported by IDIS Package 2.

NB: The meter acts as a COSEM server, the HES acts as COSEM client.

	"Open Meter" Use Case	Description	IDIS Package 2 specific remarks
UC1	Meter Registration	Process of incorporating devices (E-meters, submeters, ...) into the system.	• Registration at the HES or MDM, or DC level is performed in conjunction with the PUSH operation. • Submeters must be configured and registered.
UC2	Remote Tariff Programming	Process of remotely programming the parameters necessary to support a time of use (TOU) based tariff contract.	• Downloading and activation of TOU tables .
UC3	Meter reading (On demand) For multi-utility meters	Process of spontaneously collecting meter readings upon a specific request.	• Total/Rated-Registers • Profiles and Event-Logs
UC4	Meter reading (for billing) For multi-utility meters	Process of periodically collecting meter readings for billing purposes (periodic reading)	• Total/Rated-Registers • Profiles and Event-Logs
UC5	Disconnection and Reconnection (E, G)	Process of disconnecting or reconnecting the electricity (E) or gas (G) supply of a consumer	• Remote controlled (E,G) • Time (local) controlled (E,G) • Load (local) controlled (E)
UC6	Clock Synchronization	Process of adjusting the internal clock of the metering equipment	• For E-meters only • Source of sync HES, NTP server, Data Concentrator (where applicable)
UC7	Quality of Supply Reporting	Process of supervising Power Outages, Sags and Swells	• Event-Logs and counters • current/power/voltage instantaneous and average values
UC8	Load Management by relay (E only)	Process of controlling specific local loads by means of relays.	• Remote controlled • Time (local) controlled • Load (local) controlled
UC9	Firmware update	Process of downloading new firmware to a device	• For E-meters only • Only remote upgrade • interoperability restricted to the downloading process
UC10	Meter supervision	Process of supervising any events which could compromise the meter and the system.	• For E-meters only • Security event logs
UC11	Consumer Information	Process of periodically transmitting consumer information via a local interface	• For E-meters only
UC12	Communication Supervision	Process of supervising events affecting the meter to HES communication.	• Communication event log.

Table 2 Use Cases supported by IDIS package 2

6.1 Meter Registration

In contrast to package 1 where meter registration is part of the PLC network management in package 2 IP profile meter registration is limited to the logical registration at HES level. Establishment of the IP network connectivity is achieved following standard IP rules.

Independently of fixed or dynamic IP addressing, the IP address is typically provided to the HES (or DC) via a Push on Connectivity (comp. 8.3) operation issued by the meter.

Logical registration at HES (or DC) level is typically achieved by the valid system title of the meter provided by the Data-Notification service as defined by the Push setup – On Installation object (comp. 6.1.3).

Alternatively, logical registration at HES level may be achieved by reading the necessary data (e.g. COSEM logical device name, SAP assignment) by the Public Client.

6.1.1 System Title

Length: 8 bytes
Type: octet-string[8]

byte1	byte 2	byte 3	byte 4	byte 5		byte 6	byte 7	byte 8
MC	MC	MC	$T1_b$	$T2_b$	SN_b	SN_b	SN_b	SN_b

MC: Manufacturer Code according FLAG coded as ASCII (byte1,2,3)

$T1_b$: IDIS Meter Device Type

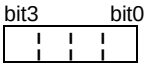
$T2_b$: IDIS Meter FunctionType

SN_b: manufacturer specific serial number (the next 28 bits, half of byte5, byte6,7,8)

The field T1/2 is used as follows:

T1 (device type):	meaning:
000...098	reserved for non-IDIS meters; system title is considered as manufacturer specific
099	reserved system title for the DC
100	IDIS package1 PLC single phase meter
101	IDIS package1 PLC polyphase meter
102	IDIS package2 IP single phase meter
103	IDIS package2 IP polyphase meter
104...255	reserved for future use

T2 (function type)	meaning:
bit0=1	Disconnector extension
bit1=1	Load Management extension
bit2=1	Multi Utility extension
bit3=0	reserved for future use by IDIS



Example System Title:

An LGZ (4c, 47, 5a) polyphase IDIS meter package 2 IP (103) with extension Disconnector and Multi Utility (0101) and with serial number 12345678 (bc,61,4e) results in the following system title (hex coded):

byte1	byte 2	byte 3	byte 4	byte 5	byte 6	byte 7	byte 8
4c	47	5a	66	50	bc	61	4e

6.1.2 COSEM Logical Device Name

Length: 16 bytes
Type: octet-string[16]

byte1	byte 2	byte 3	byte 4	byte 5	byte 6	byte 7	byte 8
MC	MC	MC	T1	T1	T1	T2	T2

byte9	byte 10	byte 11	byte 12	byte 13	byte 14	byte 15	byte 16
SN	SN	SN	SN	SN	SN	SN	SN

MC: Manufacturer Code according FLAG coded as ASCII (byte1,2,3)

T1: IDIS Device Type ASCII encoded. Meaning as in 6.1.1.

T2: IDIS Function Type ASCII encoded. Meaning as in 6.1.1.

SN: manufacturer specific serial number ASCII encoded.

Example Logical Device Name:

An LGZ polyphase IDIS meter with extension Disconnector and Multi Utility and with serial number 12345678 results in the following Logical Device Name:

byte1	byte 2	byte 3	byte 4	byte 5	byte 6	byte 7	byte 8
L	G	Z	1	0	3	0	5

byte9	byte 10	byte 11	byte 12	byte 13	byte 14	byte 15	byte 16
1	2	3	4	5	6	7	8

The COSEM Logical Device Name is accessible via the COSEM object:

COSEM Logical Device Name (class_id 1)	logical_name: 0-0:42.0.0.255

6.1.3 Meter Registration using Data-Notification

After commissioning the meter sends its IP address and its system title to the HES (or DC) using the Data-Notification service. The IDIS meter must provide a trigger (e.g. optical port, button, …) to invoke the push method of the corresponding push object (“Push setup-On Installation” LN: 0-0.25.7.8.255). The execution of the push method results in a transmission of the Data-Notification message to the set IP address destination. If the “Push setup-On Installation” object is configured for SMS communication the Data-Notification message is sent by SMS to the set telephone number destination.

Push setup – On Installation (class_id 40)	logical_name: 0-7:25.9.0.255

6.2 Remote Tariff Programming

In package 2 Remote Tariff Programming is performed in the same way as in package 1.

Tariffication is handled by instances of the following COSEM Interface classes:

- Clock (class_id: 8)
- Activity calendar (class_id 20)
- Special days table (class_id 11)
- Script table (class_id 9)
- Register activation (class_id 6)
- Register (class_id 3)
- Currently active energy tariff (class_id 1)

Figure 4 illustrates the relationship between the different COSEM objects used for tariffication.

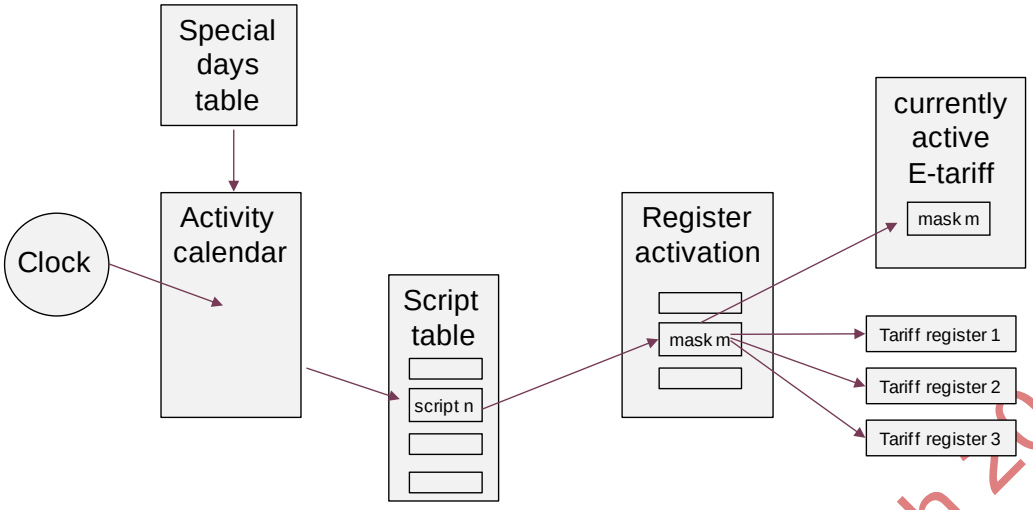


Figure 4: COSEM objects managing tariffication

In addition to the specifications provided in DLMS UA 1000-1 Ed. 12.0 the following sections provide additional information on the options supported by IDIS.

6.2.1 Activity Calendar

Tariffs are controlled by an instance of the IC “Activity Calendar” (class_id =20) with the attributes and methods as displayed below:

Activity calendar		
Attributes		*Data type used in IDIS*
logical_name	(static)	octet-string (length 6): 0-0:13.0.0.255
calendar_name_active	(static)	octet-string at least up to 8 octets
season_profile_active	(static)	array
week_profile_table_active	(static)	array
day_profile_table_active	(static)	array
calendar_name_passive	(static)	octet-string at least up to 8 octets
season_profile_passive	(static)	array
week_profile_table_passive	(static)	array
day_profile_table_passive	(static)	array
activate_passive_calendar_time	(static)	octet-string (length 12), *date_time* format

season_profile

array season (at least 4 seasons are supported by IDIS)

	season ::= structure
	{
	season_profile_name: octet-string (length 1)
	season_start: octet-string (length 12), *date_time* format
	week_name: octet-string (length 1)
	}

week_profile_table	Contains an array of exactly one week-profile per season.
	array week_profile (at least 4 entries, one per season)
	
	week_profile ::= structure
	{
	week_profile_name: octet-string (length 1)
	monday: day_id,
	tuesday: day_id,
	wednesday: day_id,
	thursday: day_id,
	friday: day_id,
	saturday: day_id,
	sunday: day_id
	}
	day_id: unsigned

day_profile_table	array day_profile (IDIS supports at least 4 entries)
	
	day_profile ::= structure
	{
	day_id: unsigned,
	day_schedule: array day_profile_action (IDIS supports at least 5 switching times per day)
	}
	
	day_profile_action ::= structure
	{
	start_time: octet-string (length 4, *time* format)
	script_logical_name: octet-string (length 6, 0-0:10.0.100.255)
	script_selector: long-unsigned
	}

activate_passive_ calendar_time	octet-string (of length 12 , *date_time* format)

6.2.2 Script table

For tariffication there is exactly one Script table

Tariffication script table (class_id 9)	logical_name: 0-0:10.0.100.255

The attribute script has at least 4 entries representing the tariffs as shown in Table 3:

Script selector	Script definition
0	NOT USED
1	Registers and actions corresponding to tariff 1 are activated
2	Registers and actions corresponding to tariff 2 are activated
3	Registers and actions corresponding to tariff 3 are activated
4	Registers and actions corresponding to tariff 4 are activated
...	Further script selectors may be used for additional tariffs

Table 3: Assignment of tariffs to scripts

6.2.2.1 Default tariff

In case of an invalid clock script 1 will be activated.

6.2.3 Register activation

Two Register activation objects are used for tariff management.

Register activation - Energy (class_id 6)	logical_name: 0-0:14.0.1.255
Register activation - Maximum Demand (class_id 6)	logical_name: 0-0:14.0.2.255

NB: If the activation of a tariff consists of more that just activating a register, then the other actions (e.g. opening/closing of relays) must be specified in the corresponding script.

6.2.4 Data: Currently active energy tariff

Currently active energy tariff (class_id 1)	logical_name: 0-0:96.14.0.255

The attribute “Value” (octet-string length 1..8) contains the “mask name” of the currently active mask of the Register Activation – Energy object.

6.2.5 Example “High and low tariff”:

HIGH Tariff is currently active

```
RegisterActivation-Energy
    Logical_name ::= 0-0:14.0.1.255
    Register_assignment ::= {
                                { class_id ::= 3, logical_name ::= 1-0:1.8.1.255},
                                { class_id ::= 3, logical_name ::= 1-0:1.8.2.255},
                                { class_id ::= 3, logical_name ::= 1-0:2.8.1.255},
                                { class_id ::= 3, logical_name ::= 1-0:2.8.2.255}
                                }
        Mask_list ::= {
                        { mask_name ::= “LOW”, index_list ::= { 1,3 } },
                        { mask_name ::= “HIGH”, index_list ::= { 2,4 } }
                }
```

Active_mask ::= “HIGH”

Currently Active Tariff
Logical_name ::= 0-0:96.14.0.255
Value ::= “HIGH”

6.2.6 Remote Tariff programming using PUSH operation

Services provided by PUSH operation are not used in this use case.

6.3 Meter Reading on Demand

While in package 1 only the GET service is used for Meter Reading on Demand, in package 2 Meter Reading on Demand may also be performed by invoking the Data-Notification service.

Precondition: if the meter is not on-line then the HES issues a wake up.

6.3.1 Electricity meter

At least the following types of registers are supported by the IDIS meter:

- 32 instances of rated registers. 16 instances must represent A+, A-, R+ and R- for 4 rates each. The remaining 16 instances are configurable by the manufacturer according to any rate defined in the Activity Calendar by considering the list of specified Total Registers defined in IDIS P2-OBJ Ed.2.0.
- 10 instances of total registers
- 20 instances of maximum demand registers
- 4 instances of demand registers

A detailed list of mandatory and optional COSEM objects supporting Meter reading can be found in IDIS P2-OBJ Ed.2.0.

6.3.1.1 Load Profiles for electricity metering

Two instances of the IC Profile Generic are supporting Electricity related registration. The status of the LP entries is encoded into 1 byte according to 6.3.4.

A detailed description of the Load Profiles for electricity metering can be found in sect. 7.4.

Load Profile 1 (1-0:99.1.0.255)

min capacity:	10 days with 15 min, 4 captured objects
structure:	clock.time, profile_status, values

capture_period	range 1-60 minutes[3], default[4] 15 minutes (900 seconds)
default captured objects:	clock.time, profile_status, A+, A-
profile_status:	according to 6.3.4
buffer encoding:	option 1[5]: normal: clock with every entry option 2: compressed: if any element can be deducted from the previous buffer entry, then the type "*null data*" (comp. DLMS UA 1000-2 Ed. 8.0:2014, p 306) is used. for values: the same as the previous for clock: previous + capture period[6]
selective access:	by range: mandatory by entry: optional
sorted method:	sorted by smallest with sort object set to 0-0:1.0.0.255 or unsorted (FIFO)

Load Profile 2 (1-0:99.2.0.255)

min capacity:	10 days with hourly entries, 4 captured objects
structure:	clock.time, profile_status, values
capture_period	typically daily (86400 seconds) capturing at midnight (local time), alternatively 1-60 min[3]
default captured objects:	clock.time, profile_status, A+, A-
profile_status:	according to 6.3.4
buffer encoding:	option 1[5] normal: clock with every entry option 2: compressed: if any element can be deducted from the previous buffer entry, then the type "*null data*" (comp. DLMS UA 1000-2 Ed. 8.0:2014, p210) is used. for values: the same as the previous for clock: previous + capture period[6]
selective access:	by range: mandatory by entry: optional
sorted method:	sorted by smallest with sort object set to 0-0:1.0.0.255 or unsorted (FIFO)

[3] IDIS meters must support at least the following values for the capture period: 5min, 10min, 15min, 30min, 60min.

[4] The meter must use/provide the „default" values during the IDIS conformance testing

[5] It's up to the meter manufacturer to equip the meter with option 1 or option 2. The HES and the MDM system must be able to handle both options.

[6] The missing time values (null data) can be deducted by the COSEM client by taking the last non-"null data" time stamp and adding a capture period for every consecutive missing time stamp. Other missing buffer values can be deducted by copying the last non-"null data" value.

6.3.2 Submeters

In IDIS up to 4 submeters may be connected to the M-Bus master in the E-meter. The metering values of each submeter are registered in a corresponding Load Profile.

6.3.2.1 M-Bus Master Load profile for channel 1..4

Up to 4 (one per M-Bus channel) M-Bus master load profiles are supported. The status of the LP entries is encoded into 1 byte according to 6.3.4 .

Load Profile M-Bus 1..4 (0-1..4:24.3.0.255)

min capacity:	10 days with hourly entries, 6 captured objects
structure:	clock time; profile_status; M-Bus Master value objects
capture_period	typically 1 hour (3600 seconds), alternatively 1-60 min[3] or daily
buffer encoding:	option 1[5]: normal: clock with every entry option 2: compressed: if any element can be deducted from the previous buffer entry, then the type "*null data*" (comp. DLMS UA 1000-2 Ed. 8.0:2014, p 306) is used. for values: the same as the previous for clock: previous + capture period[6]
selective access:	by range: mandatory by entry: optional
sorted method:	sorted by smallest with sort object set to 0-0:1.0.0.255 or unsorted (FIFO)

6.3.2.2 M-Bus Master Control log object 1..4

Up to 4 (one per M-Bus channel) control logs are supported.

Control log M-Bus 1..4 (0-1..4:24.5.0.255)

min capacity:	10
structure:	clock time; control event log
buffer encoding:	normal: clock with every entry
selective access:	by range: mandatory by entry: optional

6.3.3 Billing Profile for general metering

One instance of the IC Profile Generic is supporting Electricity and/or Multi-utility (submeters) related registration.

A more detailed description of the billing profiles can be found in sect 7.4.

Data of billing period 1 (0-0:98.1.0.255)

min capacity:	13 months with monthly billing period, 5 captured objects
structure:	clock.time, values
capture_period	0 (externally triggered via “End of billing period 1 scheduler”)
default captured objects:	clock.time, A+ rate 1;A+ rate 2; A- rate 1; A- rate 2
buffer encoding:	option 1[5]: normal: clock with every entry option 2: compressed: if any element can be deducted from the previous buffer entry, then the type “*null data*” (comp. DLMS UA 1000-2 Ed. 8.0:2014, p 306) is used. for values: the same as the previous for clock: previous + capture period[6]
selective access:	by range: mandatory by entry: optional
sorted method:	unsorted (FIFO)

6.3.4 Profile Status

The status of a buffer entry consists of a one byte (type *Unsigned*) where the bits have the meaning according to section 7.4.

6.3.5 Meter Reading on Demand using PUSH operation

PUSH operation offers the HES (or DC) the possibility to (re)trigger a Data-Notification service to retrieve missing data from the last reading period(s). If the meter is not on-line then the precondition for the triggering of the Data-Notification service is a successful wake up of the meter.

Push setup – Interval_1 (class_id 40)	logical_name: 0-1:25.9.0.255
Push setup – Interval_2 (class_id 40)	logical_name: 0-2:25.9.0.255
Push setup – Interval_3 (class_id 40)	logical_name: 0-3:25.9.0.255

6.4 Meter Reading for Billing

While in package 1 only the GET service is used for Meter Reading for Billing, in package 2 Meter Reading for Billing may also be performed by invoking the Data-Notification service.

Precondition: if the meter is not on-line then the HES issues a wake up or the push operation is triggered by the meter’s scheduler.

6.4.1 Meter Reading for Billing using PUSH operation

PUSH operation offers the possibility to periodically trigger Data-Notification services to transmit billing data to the HES (or the DC).

Push setup – Interval_1 (class_id 40)	logical_name: 0-1:25.9.0.255
Push setup – Interval_2 (class_id 40)	logical_name: 0-2:25.9.0.255
Push setup – Interval_3 (class_id 40)	logical_name: 0-3:25.9.0.255
Push action scheduler – Interval_1 (class_id 22)	logical_name: 0-1:15.0.4.255
Push action scheduler – Interval_2 (class_id 22)	logical_name: 0-2:15.0.4.255
Push action scheduler – Interval_3 (class_id 22)	logical_name: 0-3:15.0.4.255

In the Push setup objects defined above the Data-Notification message may contain: total registers, rated registers, profiles and event logs.

6.5 Meter Disconnection and Reconnection

The following section is inherited from IDIS Package 1.

Disconnection and reconnection of the electricity supply is supported by the following objects:

Disconnect Control (class_id 70)	logical_name: 0-0:96.3.10.255
Disconnect Control schedule (class_id 22)	logical_name: 0-0:15.0.1.255
Disconnector script table (class_id 9)	logical_name: 0-0:10.0.106.255
Event object disconnector (class_id 1)	logical_name: 0-0:96.11.2.255
Disconnector control log (class_id 7)	logical_name: 0-0:99.98.2.255
Limiter (class_id 71) Allows to supervise the instantaneous current or the sliding demand and executes specific actions (via script table) depending on the limits reached by the supervised values.	logical_name: 0-0:17.0.0.255
Supervision monitor x - Fuse supervision Lx (class_id 21) Allows to supervise the instantaneous or the average value of the current per phase.	L1: logical_name: 1-0:31.4.0.255 L2: logical_name: 1-0:51.4.0.255 L3: logical_name: 1-0:71.4.0.255

Disconnection and reconnection operated via an M-Bus connected submeter is supported by the following objects:

M-Bus Disconnect Control 1..4 (class_id 70)	logical_name: 0-1:24.4.0.255 logical_name: 0-2:24.4.0.255 logical_name: 0-3:24.4.0.255 logical_name: 0-4:24.4.0.255
M-Bus Disconnect Control schedule (class_id 22)[7]	logical_name: 0-1:15.0.1.255

[7] At minimum one M-bus device must be controlled with one schedule. However, if more than one M-bus devices must be controlled independently, more schedules may be added.

M-Bus Disconnector script table (class_id 9)	logical_name: 0-1:10.0.106.255
Event Objects - M-Bus Master Control logs 1..4 (class_id 1)	logical_name: 0-1:96.11.4.255 logical_name: 0-2:96.11.4.255 logical_name: 0-3:96.11.4.255 logical_name: 0-4:96.11.4.255
M-Bus master Control log object 1..4 (class_id 7)	logical_name: 0-1:24.5.0.255 logical_name: 0-2:24.5.0.255 logical_name: 0-3:24.5.0.255 logical_name: 0-4:24.5.0.255

All event logs support selective access per range. The events are enumerated from 1 to 255. The last event is always available in the corresponding event object. The event object has the value of 255 until the first event is detected/generated by the meter.

6.5.1 Disconnector script table

The disconnector script table contains the scripts which act on the Disconnect Control object 0-0:96.3.10.255 as follows:

Script identifier	Action
1	SET control_state to “Ready_for_reconnection (2)”
2	SET control_state to “Connected (1)”
3	execute method “remote_disconnect(0)”
4	execute method “remote_reconnect(0)”

The following restrictions assure conformity with DLMS UA 1000-1 Ed. 12.0. Figure 5 below is a copy of the state diagram shown in DLMS UA 1000-1 Ed. 12.0.

Script 1:
Performs a local disconnection according to transition “local_disconnect (g)” (see Figure 5). If the state transition is not allowed by the control mode, then the action is ignored.

Script 2:
Performs a local reconnection according to transition “local_reconnect (h)” (see Figure 5). If the state transition is not allowed by the control mode, then the action is ignored.

Script 3 and script 4:
With the help of the single action schedule the remote operation of the disconnector can be executed at a specific, delayed time instance. In this case the actual dis/re-connection (triggered by the single action schedule via script 3 or 4) is still interpreted as a remote operation.

The action service to method 1 “execute(data)” of the Disconnect script table object is not allowed for any remote client

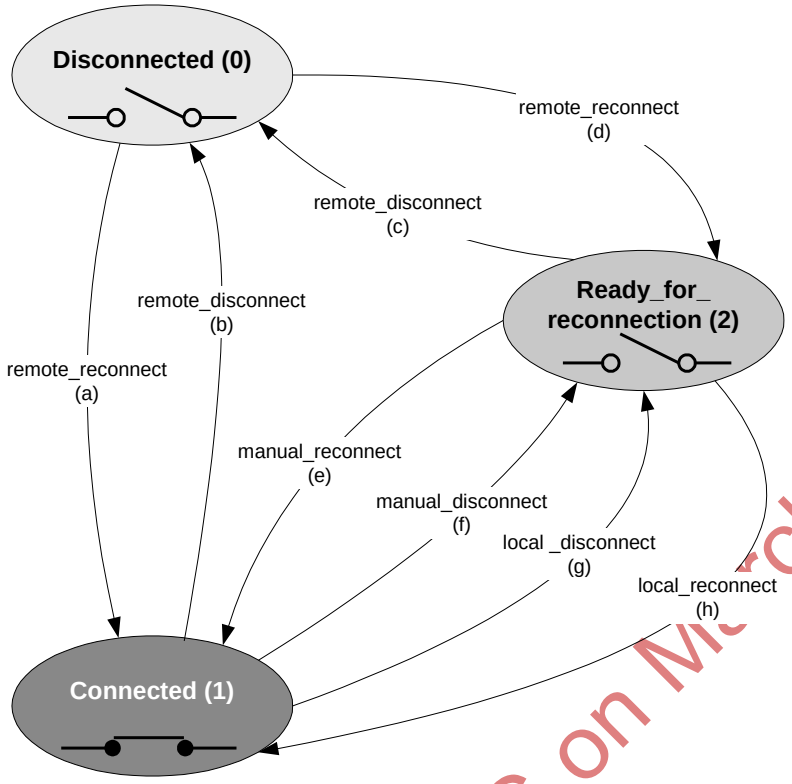


Figure 5 – State diagram of the Disconnect control IC

6.5.2 M-Bus Disconnector script table

The M-Bus disconnector script table contains the scripts which act on the M-Bus Disconnect Control objects 0-1:24.4.0.255, 0-2:24.4.0.255, 0-3:24.4.0.255 and 0-4:24.4.0.255 as follows:

Script identifier	Action
1	For M-Bus Disconnect Control 1: SET control_state to “Ready_for_reconnection (2)”
2	For M-Bus Disconnect Control 1: SET control_state to “Connected (1)”
3	For M-Bus Disconnect Control 2: SET control_state to “Ready_for_reconnection (2)”
4	For M-Bus Disconnect Control 2: SET control_state to “Connected (1)”
5	For M-Bus Disconnect Control 3: SET control_state to “Ready_for_reconnection (2)”
6	For M-Bus Disconnect Control 3: SET control_state to “Connected (1)”
7	For M-Bus Disconnect Control 4: SET control_state to “Ready_for_reconnection (2)”
8	For M-Bus Disconnect Control 4: SET control_state to “Connected (1)”
9	For M-Bus Disconnect Control 1: execute method “remote_disconnect(0)”
10	For M-Bus Disconnect Control 1: execute method “remote_reconnect(0)”
11	For M-Bus Disconnect Control 2: execute method “remote_disconnect(0)”
12	For M-Bus Disconnect Control 2: execute method “remote_reconnect(0)”
13	For M-Bus Disconnect Control 3: execute method “remote_disconnect(0)”
14	For M-Bus Disconnect Control 3: execute method “remote_reconnect(0)”
15	For M-Bus Disconnect Control 4: execute method “remote_disconnect(0)”
16	For M-Bus Disconnect Control 4: execute method “remote_reconnect(0)”

The following restrictions assure conformity with DLMS UA 1000-1 Ed. 12.0 (comp. Figure 5).

Scripts 1,3,5,7:
Performs a local disconnection according to transition “local_disconnect (g)” (see Figure 5).). If the state transition is not allowed by the control mode, then the action is ignored.

Scripts 2,4,6,8:
Performs a local reconnection according to transition “local_reconnect (h)” (see Figure 5).). If the state transition is not allowed by the control mode, then the action is ignored.

Scripts 9 to 16:

With the help of the single action schedule the remote operation of the disconnector can be executed at a specific, delayed time instance. In this case the actual dis/re-connection (triggered by the single action schedule via scripts 9 to 16) is still interpreted as a remote operation.

The action service to method 1 “execute(data)” of the M-Bus Disconnect script table object is not allowed for any remote client.

6.5.3 Meter Disconnection and Reconnection using PUSH operation

Services provided by PUSH operation are not used in this use case.

6.6 Meter Clock Synchronization

In package 2 Meter Clock Synchronization is performed in the same way as in package 1. In addition, NTP synchronization is possible as an option.

6.6.1 Mandatory Time Server: HES or DC

The time in the electricity meters is set/synchronized by applying the SET service to the attribute “time” of the “clock” object (logical_name: 0-0:1.0.0.255). In IDIS package 2 the time may be regularly set by the HES (or by the DC).

When reading the time attribute of the clock object, then the date_time field contains the information on the local time of the meter.

When setting the time attribute of the clock object then the date_time field contains the information from which the local time of the meter can be derived as shown in Table 4.

Year, month, day of month, day of week, hour, minute, second, hundredths of seconds	deviation	Clock status	Supported by the meter
the meter’s local time	0x8000 (not specified)	DST undefined: 0xFF	mandatory
the meter’s local time	0x8000 (not specified)	DST defined: 0x80/0x00	optional
local (undefined location) time	Deviation of the given (transmitted) local time to UTC	DST not active: 0x00	optional

Table 4: Time attribute in type date_time

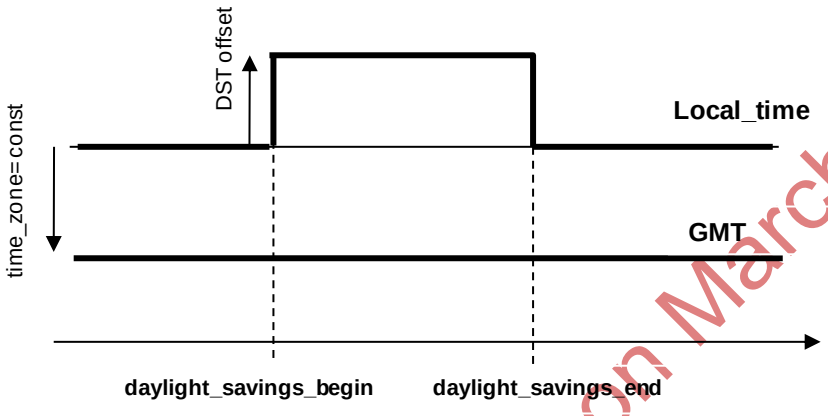
NB: When writing the time attribute, the following fields are ignored by the meter:
day of week, hundredths of seconds. The client may write these attributes explicitly or set them to “not specified” (0xFF) when writing the time.

The following rules must be considered:

Difference between new time and old time < ClockTime Shift Limit	Clock is adjusted without any further actions
Difference between new time and old time >= ClockTime Shift Limit	Clock is adjusted and “Clock Adjusted” events are triggered..

6.6.1.1 Relation between the different time parameters

The following clarifications concern the time parameters as used in DLMS UA 1000-1 Ed. 12.0



time_zone:	attribute 3 of IC Clock in minutes. It is a constant depending on the geographic location (example: Paris: -60 minutes)
deviation:	part of type ”date_time” in minutes. Is dynamic and changes depending on the time_zone and if DST is active or not. It is calculated by the server.
Local_time:	local time (current time)
DSToffset	Daylight saving time offset in minutes (”summer time” – ”winter time”)
UTC:	Greenwich Mean Time

The following relations apply:

deviation= UTC - Local_time

deviation= time_zone - DSToffset (if DST is active)

Example: Ljubljana, 13.07.2010

local:	15:00
UTC:	13:00
deviation	-120
DSToffset	+60
time_zone	-60

Clock synchronization is supported by the following objects:

Clock (class_id 8)	logical_name: 0-0:1.0.0.255
Clock Time Shift Limit (class_id 3)	logical_name: 1-0:0.9.11.255

6.6.2 Meter Clock Synchronization using PUSH operation

Services provided by PUSH operation are not used in this use case.

6.6.3 Optional Time Server: NTP

For IDIS Package 2 the meter may support an NTP client for clock synchronization as an option.

The settings for the NTP server are contained in the following objects:

NTP setup (class_id 100)	logical_name: 0-0:25.10.0.255

Clock synchronization by NTP is handled in the meter the same way as if the clock would be set by a SET service.

The NTP Time Server used in IDIS package 2 supports only the following authentication methods:

- ”shared_secrets”
- ”no secret”

NB: the support of ”shared_secrets” is mandatory. In addition, ”no secret” may be optionally supported (for backwards compatibility with existing IT infrastructure).

6.7 Quality of Supply Reporting

While in package 1 only the GET service is used for Quality of Supply Reporting, in package 2 Quality of Supply Reporting may also be performed by invoking the Data-Notification service.

Precondition: if the meter is not on-line then the HES issues a wake up or the push operation is triggered by the meter’s scheduler.

The quality of supply is reported by means of the following objects:

Power Failure Event Log (class_id 7) registering the durations of power failures in any phase	logical_name: 1-0:99.97.0.255
Power Quality Log (class_id 7)	logical_name: 0-0:99.98.4.255

registering the power quality relevant events	
Alarm Register 2[8] (class_id 3)	logical_name: 0-0:97.98.1.255
Number of Power failures in any phase (class_id 1)	logical_name: 0-0:96.7.21.255
Number of Long Power failures in any phase (class_id 1)	logical_name: 0-0:96.7.9.255
Number of Voltage Sags in Phase Lx (class_id 1), x=1,2,3	logical_name: 1-0:x.32.0.255 x=32,52,72
Number of Voltage Swells in Phase Lx (class_id 1) , x=1,2,3	logical_name: 1-0:x.36.0.255 x=32,52,72
Duration of last Voltage Sag in Phase Lx (class_id 3) , x=1,2,3	logical_name: 1-0:x.33.0.255 x=32,52,72
Duration of last Voltage Swell in Phase Lx (class_id 3) , x=1,2,3	logical_name: 1-0:x.37.0.255 x=32,52,72
Magnitude of last Voltage Sag in Phase Lx (class_id 3) , x=1,2,3	logical_name: 1-0:x.34.0.255 x=32,52,72
Magnitude of last Voltage Swell in Phase Lx (class_id 3) , x=1,2,3	logical_name: 1-0:x.38.0.255 x=32,52,72

The event identifiers are defined in IDIS P2-OBJ Ed.2.0.

All event logs support selective access per range. The events are enumerated from 1 to 255. The last event is always available in the corresponding event object. The event object has the value of 255 until the first event is detected/generated by the meter.

6.7.1 Quality of Supply Reporting using PUSH operation

PUSH operation offers the possibility to send periodically or event triggered (comp. 7.3.2) Data-Notification services to transmit Quality of Supply data to the HES.

Periodically transmitted Quality of Supply data is configured by the following objects:

Push setup – Interval_1 (class_id 40)	logical_name: 0-1:25.9.0.255
Push setup – Interval_2 (class_id 40)	logical_name: 0-2:25.9.0.255
Push setup – Interval_3 (class_id 40)	logical_name: 0-3:25.9.0.255
Push action scheduler – Interval_1 (class_id 22)	logical_name: 0-1:15.0.4.255
Push action scheduler – Interval_2 (class_id 22)	logical_name: 0-2:15.0.4.255
Push action scheduler – Interval_3 (class_id 22)	logical_name: 0-3:15.0.4.255
Push setup – On Alarm (class_id 40)	logical_name: 0-4:25.9.0.255
Push setup – On Power down (class_id 40), optional	logical_name: 0-5:25.9.0.255

The Quality of Supply data may be transferred using a *dedicated* Push setup object or it may be transferred together with other data defined in a *common* Push setup object.

[8] Package 2 features a new alarm register with extended functionality

6.8 Load Management by Relay

The following section is inherited from IDIS Package 1.

Loads may be disconnected and reconnected with the help of relay(s). The relay(s) are controlled with the following objects:

Load Management script table (class_id 9) Providing the scripts for connecting and disconnecting the relay(s) via the object Load Management Relay Control. The script table is used for local (time or event based) control of the relays.	logical_name: 0-0:10.0.103.255
Load Management - Relay control 1 (class_id 70) Providing the methods to control the relays remotely, or locally (time or event controlled) via the Load Mgt script table.	logical_name: 0-1:96.3.10.255

NB: The objects “Limiter” (0-0:17.0.0.255) and the “Supervision monitor x – Fuse supervision Lx” (1-0:31.4.0.255, 1-0:51.4.0.255, 1-0:31.4.0.255) are NOT used to control the relays.

6.8.1 Load Management script table

The Load Management script table contains the scripts which act on the Load Management – Relay Control object 0-1:96.3.10.255 as follows:

Script identifier	Action
1	SET control_state to “Ready_for_reconnection (2)”
2	SET control_state to “Connected (1)”
3	execute method “remote_disconnect(0)”
4	execute method “remote_reconnect(0)”

The following restrictions assure conformity with DLMS UA 1000-1 Ed. 12.0 (comp. Figure 5).

Script 1:
Performs a local disconnection according to transition “local_disconnect (g)” (see Figure 5). If the state transition is not allowed by the control mode, then the action is ignored.

Script 2:
Performs a local reconnection according to transition “local_reconnect (h)” (Figure 5). If the state transition is not allowed by the control mode, then the action is ignored.

Script 3 and script 4:
With the help of the single action schedule the remote operation of the disconnector can be executed at a specific, delayed time instance. In this case the actual dis/re-connection (triggered by the single action schedule via script 3 or 4) is still interpreted as a remote operation.

The action service to method 1 “execute(data)” of the Load Management script table is *not allowed* for any remote client

6.8.2 Load Management by Relay using PUSH operation

Services provided by PUSH operation are not used in this use case.

6.9 Firmware Update

The following section is inherited from IDIS Package 1.

The raw image for firmware download must be provided to the COSEM client as a binary file. The COSEM client then uses the services provided by the objects listed below to transfer the binary file into the meter and to activate the new firmware.

Image transfer (class_id 18)	logical_name: 0-0:44.0.0.255
Image transfer activation scheduler (class_id 22)	logical_name: 0-0:15.0.2.255
Predefined Scripts - Image activation (class_id 9)	logical_name: 0-0:10.0.107.255
Active firmware identifier (class_id 1)	logical_name: 1-0:0.2.0.255
Active firmware version signature (class_id 1)	logical_name: 1-0:0.2.8.255

Remark:

If the metrological part of the firmware *is not* separated from the rest, then the B field in the logical_name of the Active firmware version and the Active firmware version signature is set B=0.

If the metrological part of the firmware *is* separated then the B field in the logical_name of the Active firmware version and the Active firmware version signature is set as follows:

- B=0 Metrologically relevant part of firmware
- B=1...9 to identify other parts of firmware

6.9.1 Firmware Update using PUSH operation

Services provided by PUSH operation are not used in this use case.

6.10 Meter Supervision

While in package 1 only the GET service is used for Meter Supervision, in package 2 Meter Supervision may also be performed by invoking the Data-Notification service.

Precondition: if the meter is not on-line then the HES issues a wake up or the push operation is triggered by the meter's scheduler.

The meter automatically supervises critical actions and logs them in the corresponding objects.

Standard Event log (class_id 7) Containing event codes. At least 100 entries are supported.	logical_name: 0-0:99.98.0.255
Fraud Detection log (class_id 7) Containing fraud event codes. At least 30 entries are supported.	logical_name: 0-0:99.98.1.255
Alarm Register 1 (class_id 3)	logical_name: 0-0:97.98.0.255
Alarm Register 2 (class_id 3)	logical_name: 0-0:97.98.1.255

The event identifiers are defined in IDIS P2-OBJ Ed.2.0.

All event logs support selective access per range. The events are enumerated from 1 to 255. The last event is always available in the corresponding event object. The event object has the value of 255 until the first event is detected/generated by the meter.

6.10.1 Meter Supervision using PUSH operation

PUSH operation offers the possibility to send periodically or event triggered (comp. 7.3.2) Data-Notification services to transmit Meter Supervision data to the HES (or to the DC).

Periodically transmitted Meter Supervision data is configured by the following objects where the Meter Supervision data is added next to the Billing data:

Push setup – Interval_1 (class_id 40)	logical_name: 0-1:25.9.0.255
Push setup – Interval_2 (class_id 40)	logical_name: 0-2:25.9.0.255
Push setup – Interval_3 (class_id 40)	logical_name: 0-3:25.9.0.255
Push action scheduler – Interval_1 (class_id 22)	logical_name: 0-1:15.0.4.255
Push action scheduler – Interval_2 (class_id 22)	logical_name: 0-2:15.0.4.255
Push action scheduler – Interval_3 (class_id 22)	logical_name: 0-3:15.0.4.255

Event triggered transmission of the Meter Supervision data is configured by the following objects:

Push setup – On Alarm (class_id 40)	logical_name: 0-4:25.9.0.255

6.11 Consumer Information Push (CIP) using PUSH operation

In conjunction with PUSH operation IDIS package 2 meters may support the provision of local Consumer Information (as an option). This information consists of a predefined set of attributes

which are periodically transmitted to a local port serving as Consumer Information Interface (CII). Depending on the market request, this local port may be connected to a suitable home gateway.

However, the specification of the home gateway and the binding of any external device to the meter is not in the scope of IDIS package 2.

6.11.1 Client - Server structure for the optional CIP client

In order to support the optional CIP functionality the general Client Server architecture described in **section 8.1** is extended with a CIP client as shown in Figure 6.

The Consumer Information Push (CIP) shall use a dedicated Client [**103**] with at minimum Data-Notification service supported. The Client is **pre-established** and has its own security context.

For Conformance testing:

- CIP Client related tests are only performed if the optional CIP functionality is supported in an IDIS DUT. The availability of the CIP functionality must be declared in the CTI.
- The local port must be identified by the manufacturer and the manufacturer must provide a suitable converter allowing the COM port of the IDIS test tool to be connected to the local port of the DUT.

Foreseen communication is **one way only** i.e. Push from Server [1] to Client [103].

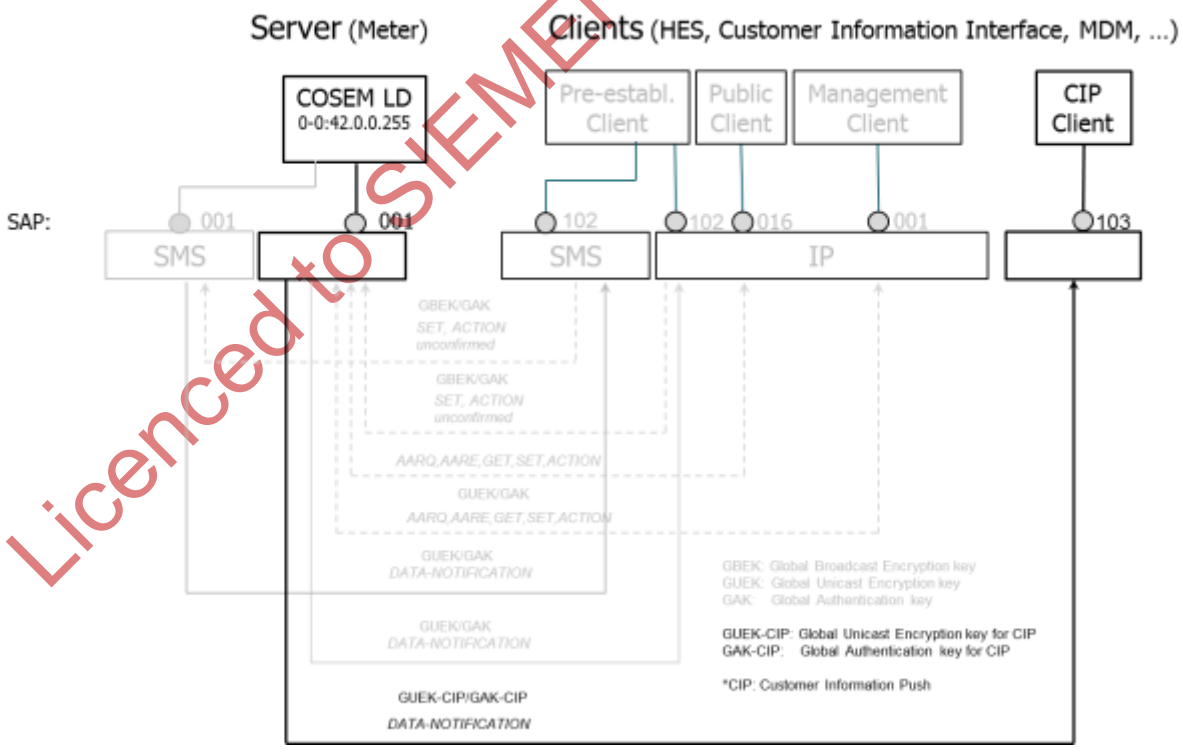


Figure 6: IDIS Client-Server structure with the optional CIP Client

6.11.2 CIP protocol stack

6.11.2.1 HDLC based protocol stack

- The protocol stack is of three layer collapsed type.
- Frame type 3 and the non-basic frame format transparency according to IEC 13239, sect. 4.3.3 is used.
- The meter acts as HDLC primary/control station according to IEC 13239 (sect. 6.13 Unbalanced connectionless operation).
- The control station sends unsolicited UI frames carrying the data as configured in the PUSH setup.
- According to IEC 13239 sect. 6.13.4.2.1: whenever the control station is ready to send a UI command frame, it shall send it immediately since there is no flow control in connectionless class service. The tributary station(s) shall only send UI response frames when given permission to do so.
- The connection is unidirectional from meter to client 103 and therefore the meter never gives permission to the tributary station to UI responses.

6.11.2.2 IP based protocol stack

- For a CIP interface supporting IP communication the architecture shown in Figure 2 (right hand side) is used.
- The transport layer is restricted to UDP.
- The default UDP Port is DLMS/COSEM UDP Port 4059

6.11.3 Security on the Consumer Information Interface

The data *from the meter* pushed to the CII (via CIP) may be secured (encryption and/or authentication) *by the meter*.

- If it is secured, then security suite 0 is applied.
- The security material used for this Meter-CII- ConsumerEquipment communication is independent of the security material used for the remote Meter-HES communication.

The CIP security context is defined in a dedicated security setup object (according to 9.4.)

The keys (CIP keys) used for the data pushed to the CII are managed by the HES (comp. Figure 7) . To change a CIP key:

1. the HES wraps the new CIP key with the meter's master key,
2. the HES sends the wrapped key to the meter using the method global_key_transfer of the object "Security setup-Consumer Information" (logical_name: 0-0:43.0.1.255) via the Management Client association.

The delivery of the appropriate key to the consumer equipment (user of the CII) is out of scope of IDIS Package 2.

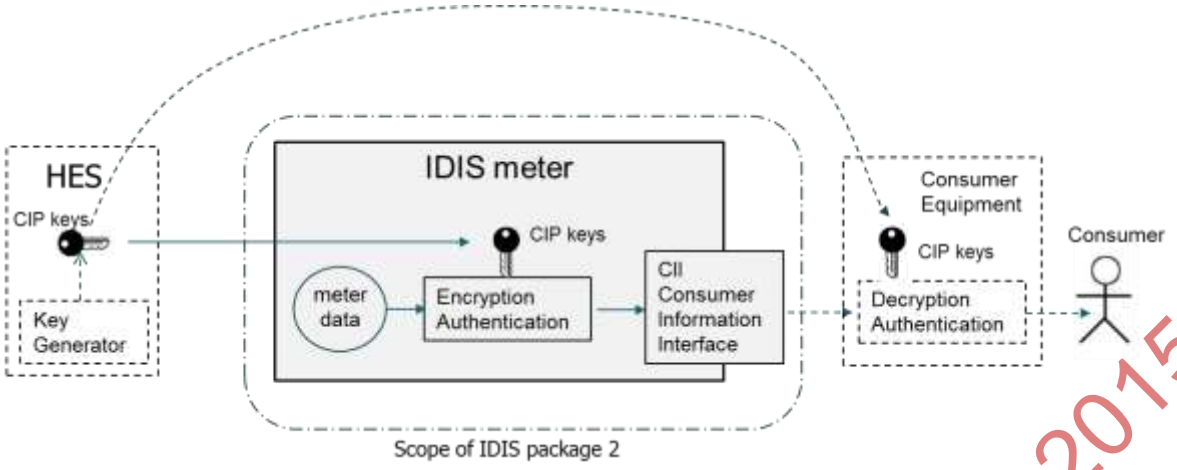


Figure 7: Managing the CIP keys

The **CIP frame counters** used for the data pushed to the CII are not accessible from outside the meter (neither by the HES nor by the consumer equipment). Upon reception of a new set of keys from the HES the meter resets the CIP frame counters .The meter increments the frame counter with every message pushed.

The Consumer equipment is expected[9] to perform the frame counter validation on every message received according to the following validation rule:

- After the consumer equipment receives a new set of global keys it will accept the first message (assuming that is encoded/authenticated with the right key) independent of the value of the frame counter. The value of the received first frame counter is then used as “initial” frame counter value.
- All the following messages are only accepted if the frame counter of the currently received message is larger than the frame counter of the previously received message.

6.11.4 CIP System Title and Error Handling

- The System title used for the CIP communication is the Meter's system title.
- The Error handling for the CII to consumer equipment communication is not in the scope IDIS Package 2.

6.11.5 Object model and Use cases covered

[9] The specification of the consumer equipment is not in the scope of IDIS package 2.

Instance name	IC	OBIS	Use Case
Consumer Message Text - Consumer Information	1	0-0:96.13.0.255	Sending a text message from HES to the Consumer Information interface (CII). The HES accesses the register on the meter via Management Client [1] or Pre-established Client [102]. The meter will - immediately after receiving the message - forward the data to the CII via the Consumer Information Push to the CIP client [103] using the Data-Notification service.

If the optional CIP functionality is supported then the following objects are mandatory:

Instance name	IC	OBIS	Use Case
Push action scheduler - Consumer Information	22	0-4:15.0.4.255	Defines the time instances (by default every 15sec) when the meter is pushing information (as set in Push setup) to the CII (CIP Client 103). The HES may access the settings of the scheduler via the Management Client. The single action schedule is of type 5. with an array of n-execution times in order to provide enough granularity of scheduled action. The scheduler's executed_script references the Push script table [0-0:10.0.108.255].
Push setup - Consumer Information	40	0-6:25.9.0.255	Definition of the set of data the meter will push to the CII. The data will be pushed according to the corresponding push action scheduler execution_time.
Security setup - Consumer Information	64	0-0:43.0.1.255	Security setup instance managing the global keys used to secure the meter data pushed to the CII (via CIP).
HDLC CIP port	23	0-1:22.0.0.255	CIP HDLC configuration

Table 5: Mandatory COSEM objects for IDIS meters supporting the optional CIP functionality

6.12 Communication Supervision

The meter automatically supervises critical events concerning the WAN and the NN (in case of G3 communication) connectivity and logs them in the corresponding objects.

Communication Log (class_id 7) Containing communication event codes. At least 100 entries are supported..	logical_name: 0-0:99.98.5.255
Event Object - Communication Log (class_id 1)	logical_name: 0-0:96.11.5.255

The event identifiers are defined in IDIS P2-OBJ Ed.2.0. (a copy can be found in section 10).

The Communication Log supports selective access per range. The events are enumerated from 1 to 255. The last event is always available in the corresponding event object. The event object has the value of 255 until the first event is detected/generated by the meter.

7. E-Meter Functionality

7.1 Data Model

The entire functionality of the IDIS meter is modeled by means of COSEM objects as described in DLMS UA 1000-1 Ed. 12.0.

IDIS P2-OBJ Ed.2.0 provides a complete list of the mandatory and optional objects used in IDIS package 2. The objects are described in all details, in particular:

- explicit type definition of the attributes;
- default values[4] of the attributes;
- specific access rights (GET, SET, ACTION) per attribute or method and per client (Public, Pre-established, Management);

An IDIS server must support ALL IDIS objects, attributes, methods and ranges of attributes (mandatory and optional) as defined in IDIS P2-OBJ Ed.2.0.

7.2 IDIS Meter customization

Every IDIS meter must support the complete set of BASIC objects. Further, the minimal (basic) functionality may be extended with any combination of:

- Disconnector,
- Load Management,
- Multi-Utility functionality,

In all cases the IDIS meter must support all *mandatory objects* in the set of the corresponding extension.

The implemented extensions become part of the IDIS test label (see 4).

In addition, the manufacturer of an IDIS meter may implement also *optional objects* (comp. IDIS P2-OBJ Ed.2.0). The *optional objects* must be identified for the IDIS conformance testing and will be listed in the test report.

7.2.1 BASIC objects

The following (comp. Table 6) COSEM objects are mandatory for every IDIS package 2 device. Not all rated registers are mandatory. For details on the mandatory rated registers comp. 6.3.1.

Instance Name	OBIS	IC
SAP Assignment	0-0:41.0.0.255	17
Current association	0-0:40.0.0.255	15
Security setup	0-0:43.0.0.255	64
Security - Receive frame counter - broadcast key	0-0:43.1.1.255	1

Instance Name	OBIS	IC
Security - Receive frame counter - unicast key	0-0:43.1.0.255	1
COSEM logical device name	0-0:42.0.0.255	1
Device ID 1, manufacturing number	0-0:96.1.0.255	1
Device ID 2	0-0:96.1.1.255	1
Device ID 3	0-0:96.1.2.255	1
Device ID 4	0-0:96.1.3.255	1
Device ID 5	0-0:96.1.4.255	1
Device ID 6: IDIS certification number	0-0:96.1.5.255	1
Currently active energy tariff	0-0:96.14.0.255	1
Clock	0-0:1.0.0.255	8
Clock Time Shift Limit	1-0:0.9.11.255	3
Activity Calendar	0-0:13.0.0.255	20
Special Days Table	0-0:11.0.0.255	11
Register activation - Energy	0-0:14.0.1.255	6
Register activation - Maximum Demand	0-0:14.0.2.255	6
Tariffication script table	0-0:10.0.100.255	9
Predefined Scripts - MDI reset / end of billing period	0-0:10.0.1.255	9
End of billing period 1 scheduler	0-0:15.0.0.255	22
Data of billing period 1	0-0:98.1.0.255	7
Error Register[10]	0-0:97.97.0.255	1
Alarm Register 1	0-0:97.98.0.255	1
Alarm Register 2	0-0:97.98.1.255	1
Alarm Filter	0-0:97.98.10.255	1
Alarm Filter 2	0-0:97.98.11.255	1
Event Object - Standard Event Log	0-0:96.11.0.255	1
Standard Event Log	0-0:99.98.0.255	7
Event Object - Fraud Detection Log	0-0:96.11.1.255	1
Fraud Detection Log	0-0:99.98.1.255	7
Consumer Message Text	0-0:96.13.0.255	1
Consumer Message Code	0-0:96.13.1.255	1
Image transfer	0-0:44.0.0.255	18
Image transfer activation scheduler	0-0:15.0.2.255	22
Predefined Scripts - Image activation	0-0:10.0.107.255	9
Active firmware version	1-0:0.2.0.255	1
Active firmware version signature	1-0:0.2.8.255	1

[10] The meaning of the Error Register bits is the same as for the Alarm Register 1 (comp. 7.3.2.3)

Instance Name	OBIS	IC
Active energy import (+A)	1-0:1.8.0.255	3
Active energy export (−A)	1-0:2.8.0.255	3
Active energy (|+A|+|-A|) Combined total	1-0:15.8.0.255	3
Active energy (|+A|-|-A|) Combined total	1-0:16.8.0.255	3
Reactive energy QI (+Ri)	1-0:5.8.0.255	3
Reactive energy QII (+Rc)	1-0:6.8.0.255	3
Reactive energy QIII (-Ri)	1-0:7.8.0.255	3
Reactive energy QIV (-Rc)	1-0:8.8.0.255	3
Reactive energy import (+R) (QI+QII)	1-0:3.8.0.255	3
Reactive energy export (-R) (QIII+QIV)	1-0:4.8.0.255	3
Active energy import (+A) rate 1	1-0:1.8.1.255	3
Active energy import (+A) rate 2	1-0:1.8.2.255	3
Active energy import (+A) rate 3	1-0:1.8.3.255	3
Active energy import (+A) rate 4	1-0:1.8.4.255	3
Active energy export (−A) rate 1	1-0:2.8.1.255	3
Active energy export (−A) rate 2	1-0:2.8.2.255	3
Active energy export (−A) rate 3	1-0:2.8.3.255	3
Active energy export (−A) rate 4	1-0:2.8.4.255	3
Reactive energy (+R) rate 1	1-0:3.8.1.255	3
Reactive energy (+R) rate 2	1-0:3.8.2.255	3
Reactive energy (+R) rate 3	1-0:3.8.3.255	3
Reactive energy (+R) rate 4	1-0:3.8.4.255	3
Reactive energy (-R) rate 1	1-0:4.8.1.255	3
Reactive energy (-R) rate 2	1-0:4.8.2.255	3
Reactive energy (-R) rate 3	1-0:4.8.3.255	3
Reactive energy (-R) rate 4	1-0:4.8.4.255	3
Reactive energy (QI) rate 1	1-0:5.8.1.255	3
Reactive energy (QI) rate 2	1-0:5.8.2.255	3
Reactive energy (QI) rate 3	1-0:5.8.3.255	3
Reactive energy (QI) rate 4	1-0:5.8.4.255	3
Reactive energy (QII) rate 1	1-0:6.8.1.255	3
Reactive energy (QII) rate 2	1-0:6.8.2.255	3
Reactive energy (QII) rate 3	1-0:6.8.3.255	3
Reactive energy (QII) rate 4	1-0:6.8.4.255	3
Reactive energy (QIII) rate 1	1-0:7.8.1.255	3
Reactive energy (QIII) rate 2	1-0:7.8.2.255	3
Reactive energy (QIII) rate 3	1-0:7.8.3.255	3

Instance Name	OBIS	IC
Reactive energy (QIII) rate 4	1-0:7.8.4.255	3
Reactive energy (QIV) rate 1	1-0:8.8.1.255	3
Reactive energy (QIV) rate 2	1-0:8.8.2.255	3
Reactive energy (QIV) rate 3	1-0:8.8.3.255	3
Reactive energy (QIV) rate 4	1-0:8.8.4.255	3
Demand Register 1 - Active energy import (+A)	1-0:1.4.0.255	5
Demand Register 2 - Active energy export (−A)	1-0:2.4.0.255	5
Demand Register 3 - Reactive energy import (+R)	1-0:3.4.0.255	5
Demand Register 4 - Reactive energy export (-R)	1-0:4.4.0.255	5
Maximum Demand Register 1 - Active energy import (+A)	1-0:1.6.0.255	4
Maximum Demand Register 2 - Active energy import (+A) - rate 1	1-0:1.6.1.255	4
Maximum Demand Register 3 - Active energy import (+A) - rate 2	1-0:1.6.2.255	4
Maximum Demand Register 4 - Active energy import (+A) - rate 3	1-0:1.6.3.255	4
Maximum Demand Register 5 - Active energy import (+A) - rate 4	1-0:1.6.4.255	4
Maximum Demand Register 6 - Active energy export (−A)	1-0:2.6.0.255	4
Maximum Demand Register 7 - Active energy export (−A) - rate 1	1-0:2.6.1.255	4
Maximum Demand Register 8 - Active energy export (−A) - rate 2	1-0:2.6.2.255	4
Maximum Demand Register 9 - Active energy export (−A) - rate 3	1-0:2.6.3.255	4
Maximum Demand Register 10 - Active energy export (−A) - rate 4	1-0:2.6.4.255	4
Maximum Demand Register 11 - Reactive energy import (+R)	1-0:3.6.0.255	4
Maximum Demand Register 12 - Reactive energy import (+R) - rate 1	1-0:3.6.1.255	4
Maximum Demand Register 13 - Reactive energy import (+R) - rate 2	1-0:3.6.2.255	4
Maximum Demand Register 14 - Reactive energy import (+R) - rate 3	1-0:3.6.3.255	4
Maximum Demand Register 15 - Reactive energy import (+R) - rate 4	1-0:3.6.4.255	4
Maximum Demand Register 16 - Reactive energy export (-R)	1-0:4.6.0.255	4
Maximum Demand Register 17 - Reactive energy export (-R) - rate 1	1-0:4.6.1.255	4
Maximum Demand Register 18 - Reactive energy export (-R) - rate 2	1-0:4.6.2.255	4
Maximum Demand Register 19 - Reactive energy export (-R) - rate 3	1-0:4.6.3.255	4
Maximum Demand Register 20 - Reactive energy export (-R) - rate 4	1-0:4.6.4.255	4
Profile status - Load profile with period 1	0-0:96.10.1.255	1
Load profile with period 1 i.e. General Load Profile	1-0:99.1.0.255	7
Profile status - Load profile with period 2	0-0:96.10.2.255	1
Load profile with period 2 i.e. Daily Values Profile	1-0:99.2.0.255	7
Number of power failures in any phase	0-0:96.7.21.255	1
Number of long power failures in any phase	0-0:96.7.9.255	1
Time threshold for long power failure	0-0:96.7.20.255	3
Duration of last long power failure in any phase	0-0:96.7.19.255	3

Instance Name	OBIS	IC
Threshold for voltage sag	1-0:12.31.0.255	3
Time threshold for voltage sag	1-0:12.43.0.255	3
Number of voltage sags in phase L1	1-0:32.32.0.255	1
Number of voltage sags in phase L2	1-0:52.32.0.255	1
Number of voltage sags in phase L3	1-0:72.32.0.255	1
Duration of last voltage sag in phase L1	1-0:32.33.0.255	3
Duration of last voltage sag in phase L2	1-0:52.33.0.255	3
Duration of last voltage sag in phase L3	1-0:72.33.0.255	3
Magnitude of last voltage sag in phase L1	1-0:32.34.0.255	3
Magnitude of last voltage sag in phase L2	1-0:52.34.0.255	3
Magnitude of last voltage sag in phase L3	1-0:72.34.0.255	3
Threshold for voltage swell	1-0:12.35.0.255	3
Time threshold for voltage swell	1-0:12.44.0.255	3
Number of voltage swells in phase L1	1-0:32.36.0.255	1
Number of voltage swells in phase L2	1-0:52.36.0.255	1
Number of voltage swells in phase L3	1-0:72.36.0.255	1
Duration of last voltage swell in phase L1	1-0:32.37.0.255	3
Duration of last voltage swell in phase L2	1-0:52.37.0.255	3
Duration of last voltage swell in phase L3	1-0:72.37.0.255	3
Magnitude of last voltage swell in phase L1	1-0:32.38.0.255	3
Magnitude of last voltage swell in phase L2	1-0:52.38.0.255	3
Magnitude of last voltage swell in phase L3	1-0:72.38.0.255	3
Threshold for missing voltage (voltage cut)	1-0:12.39.0.255	3
Time threshold for voltage cut	1-0:12.45.0.255	3
Power Failure Event Log	1-0:99.97.0.255	7
Event Object - Power Quality Log	0-0:96.11.4.255	1
Power Quality Log	0-0:99.98.4.255	7
Instantaneous voltage L1	1-0:32.7.0.255	3
Average voltage L1	1-0:32.24.0.255	3
Instantaneous current L1	1-0:31.7.0.255	3
Instantaneous voltage L2	1-0:52.7.0.255	3
Average voltage L2	1-0:52.24.0.255	3
Instantaneous current L2	1-0:51.7.0.255	3
Instantaneous voltage L3	1-0:72.7.0.255	3
Average voltage L3	1-0:72.24.0.255	3
Instantaneous current L3	1-0:71.7.0.255	3
Instantaneous current (sum over all phases)	1-0:90.7.0.255	3

Instance Name	OBIS	IC
Instantaneous active power (|+A|+|-A|)	1-0:15.7.0.255	3
Instantaneous active import power (+A)	1-0:1.7.0.255	3
Instantaneous active export power (-A)	1-0:2.7.0.255	3
Instantaneous reactive import power (+R)	1-0:3.7.0.255	3
Instantaneous reactive export power (-R)	1-0:4.7.0.255	3
IEC HDLC setup - HDLC Optical port	0-0:22.0.0.255	23
Communication Log	0-0:99.98.5.255	7
Event Object - Communication Log	0-0:96.11.5.255	1

Table 6: General BASIC (mandatory) IDIS objects

Table 7 shows the PUSH specific BASIC (mandatory) objects.

Instance Name	OBIS	IC
Push setup – On Connectivity, Auto answer	0-0:25.9.0.255	40
Push setup - On Alarm, trigger Alarm monitor 1 or 2	0-4:25.9.0.255	40
Push setup - On Installation, trigger “commissioning event”	0-7:25.9.0.255	40
Push script table	0-0:10.0.108.255	9
Alarm monitor 1	0-0:16.1.0.255	21
Alarm monitor 2	0-0:16.1.1.255	21
Alarm Descriptor 1	0-0:97.98.20.255	1
Alarm Descriptor 2	0-0:97.98.21.255	1
Push setup - Interval_1, trigger Push action scheduler - Interval_1	0-1:25.9.0.255	40
Push setup - Interval_2, trigger Push action scheduler - Interval_2	0-2:25.9.0.255	40
Push setup - Interval_3, trigger Push action scheduler - Interval_3	0-3:25.9.0.255	40
Push action scheduler - Interval_1	0-1:15.0.4.255	22
Push action scheduler - Interval_2	0-2:15.0.4.255	22
Push action scheduler - Interval_3	0-3:15.0.4.255	22

Table 7: PUSH specific BASIC (mandatory) IDIS objects

Remark:
The parameters of the attribute “scripts” of the *Push script table* (comp.DLMS UA 1000-1 Ed. 12.0) are defined as follows:

Script_identifier	service_id	class_id	logical_name	Index	parameter
1	2	40	0-1:25.9.0.255	1	0
2	2	40	0-2:25.9.0.255	1	0
3	2	40	0-3:25.9.0.255	1	0
4	2	40	0-4:25.9.0.255	1	0
5	2	40	0-0:25.9.0.255	1	0
6	2	40	0-7:25.9.0.255	1	0
7	2	40	0-5:25.9.0.255	1	0
8	2	40	0-6:25.9.0.255	1	0

The objects shown in Table 8 are also PUSH specific, but they are optional (comp. IDIS P2-OBJ Ed.2.0).

Instance Name	OBIS	IC
Push setup - On Power down, *Power down implicitly (optional)*	0-5:25.9.0.255	40
Push setup – Consumer Information, *trigger Push action scheduler – Consumer Information*	0-6:25.9.0.255	40
Push action scheduler – Consumer Information	0-4:15.0.4.255	22

Table 8 PUSH specific optional objects

Other elements and objects needed to cover use cases as described above are a part of BASIC functionality and are mandatory for all IDIS Package 2 meters (see Table 7)

7.2.1.1 Communication profile and media specific objects

Table 9 shows the Communication Profile specific BASIC (*mandatory)* objects.

Instance Name	OBIS	IC
TCP-UDP setup	0-0:25.0.0.255	41
IPv4 setup	0-0:25.1.0.255	42
IPv6 setup (alternatively to IPv4)	0-0:25.7.0.255	48

Table 9: Communication Profile specific BASIC (mandatory) objects

- The instance of TCP-UDP setup is mandatory
- At least one instance of IPv4 setup or IPv6 setup must be present.
- The attribute DL_reference of the IPv4/IPv6 setup objects specifies which internet access medium is used. All objects supporting the specified access medium are mandatory and they become part of the conformance test. Any medium specific tests are done based on the value of DL_reference and on the declarations in the CTI file.
- If the IDIS meter provides several separated IP ports then more than one instance of the setup classes is required. In this case the B field of the OBIS code is incremented by 1 for each new instance.

Table 10 contains the access medium specific objects must be available in an IDIS meter supporting internet access via GPRS and/or Ethernet or G3. For conformance testing the access medium must be declared in the CTI file.

Instance Name	OBIS	IC
Mandatory instances for access medium GPRS		
PPP setup	0-0:25.3.0.255	44
GPRS modem setup	0-0:25.4.0.255	45
Modem configuration	0-0:2.0.0.255	27
Auto answer	0-0:2.2.0.255	28
Auto connect	0-0:2.1.0.255	29
Mandatory instances for access medium Ethernet		
MAC address setup	0-0:25.2.0.255	43
Auto connect	0-0:2.1.0.255	29
Mandatory instances for access medium G3		
G3-PLC MAC layer counters	0-0:29.0.0.255	90
G3-PLC MAC setup	0-0:29.1.0.255	91
G3-PLC MAC 6LoWPAN adaptation layer setup	0-0:29.2.0.255	92
MAC address setup	0-0:25.2.0.255	43
Auto connect	0-0:2.1.0.255	29

Table 10: Access medium specific BASIC objects

If the meter connects to the internet via another access medium suitable for conformance testing then this has to be declared in the CTI file.

7.2.2 Extension D objects

The following (comp. Table 11) objects are foreseen for all IDIS devices supporting the Disconnector functionality. Detailed information on mandatory/optional objects and attributes can be found in IDIS P2-OBJ Ed.2.0.

Instance Name	OBIS	IC
Disconnect control scheduler	0-0:15.0.1.255	22
Disconnector script table	0-0:10.0.106.255	9
Disconnect control	0-0:96.3.10.255	70
Event Object - Disconnector Control log	0-0:96.11.2.255	1
Disconnector Control Log	0-0:99.98.2.255	7
Limiter	0-0:17.0.0.255	71
Supervision monitor 1 - Fuse supervision L1	1-0:31.4.0.255	21
Supervision monitor 2 - Fuse supervision L2	1-0:51.4.0.255	21

Instance Name	OBIS	IC
Supervision monitor 3 - Fuse supervision L3	1-0:71.4.0.255	21
Sliding Average current L1 (for fuse supervision)	1-0:31.4.0.255	5
Sliding Average current L2 (for fuse supervision)	1-0:51.4.0.255	5
Sliding Average current L3 (for fuse supervision)	1-0:71.4.0.255	5
Average Import Power (+A)	1-0:1.24.0.255	5
Average Net Power (|+A|-|-A|)	1-0:16.24.0.255	5
Average Total Power (|+A|+|-A|)	1-0:15.24.0.255	5

Table 11: Extension D IDIS objects

7.2.3 Extension L objects

The following objects (comp. Table 12) are foreseen for all IDIS devices supporting the Load Management functionality. Detailed information on mandatory/optional objects and attributes can be found in IDIS P2-OBJ Ed.2.0.

Instance Name	OBIS	IC
Load Mgmt script table	0-0:10.0.103.255	9
Load Mgmt - Relay control 1	0-1:96.3.10.255	70
Load Mgmt - Relay control 2	0-2:96.3.10.255	70

Table 12: Extension L IDIS objects

7.2.4 Extension M objects

The following objects (comp. Table 13) are foreseen for all IDIS devices supporting the Multi-Utility (restricted to M-bus for IDIS package 2) functionality. Detailed information on mandatory/optional objects and attributes can be found in IDIS P2-OBJ Ed.2.0.

Instance Name	OBIS	IC
M-Bus master port setup 1	0-0:24.6.0.255	74
M-Bus client channel 1	0-1:24.1.0.255	72
M-Bus client channel 2	0-2:24.1.0.255	72
M-Bus client channel 3	0-3:24.1.0.255	72
M-Bus client channel 4	0-4:24.1.0.255	72
M-Bus Value channel 1, instance 1	0-1:24.2.1.255	4
M-Bus Value channel 1, instance 2	0-1:24.2.2.255	4
M-Bus Value channel 1, instance 3	0-1:24.2.3.255	4
M-Bus Value channel 1, instance 4	0-1:24.2.4.255	4
M-Bus Value channel 2, instance 1	0-2:24.2.1.255	4
M-Bus Value channel 2, instance 2	0-2:24.2.2.255	4

M-Bus Value channel 2, instance 3	0-2:24.2.3.255	4
M-Bus Value channel 2, instance 4	0-2:24.2.4.255	4
M-Bus Value channel 3, instance 1	0-3:24.2.1.255	4
M-Bus Value channel 3, instance 2	0-3:24.2.2.255	4
M-Bus Value channel 3, instance 3	0-3:24.2.3.255	4
M-Bus Value channel 3, instance 4	0-3:24.2.4.255	4
M-Bus Value channel 4, instance 1	0-4:24.2.1.255	4
M-Bus Value channel 4, instance 2	0-4:24.2.2.255	4
M-Bus Value channel 4, instance 3	0-4:24.2.3.255	4
M-Bus Value channel 4, instance 4	0-4:24.2.4.255	4
M-Bus Device ID 1 channel 1	0-1:96.1.0.255	1
M-Bus Device ID 1 channel 2	0-2:96.1.0.255	1
M-Bus Device ID 1 channel 3	0-3:96.1.0.255	1
M-Bus Device ID 1 channel 4	0-4:96.1.0.255	1
M-Bus Device ID 2 channel 1	0-1:96.1.1.255	1
M-Bus Device ID 2 channel 2	0-2:96.1.1.255	1
M-Bus Device ID 2 channel 3	0-3:96.1.1.255	1
M-Bus Device ID 2 channel 4	0-4:96.1.1.255	1
Profile status for M-Bus Master Load profile 1	0-1:96.10.3.255	1
Profile status for M-Bus Master Load profile 2	0-2:96.10.3.255	1
Profile status for M-Bus Master Load profile 3	0-3:96.10.3.255	1
Profile status for M-Bus Master Load profile 4	0-4:96.10.3.255	1
M-Bus Master Load profile for channel 1	0-1:24.3.0.255	7
M-Bus Master Load profile for channel 2	0-2:24.3.0.255	7
M-Bus Master Load profile for channel 3	0-3:24.3.0.255	7
M-Bus Master Load profile for channel 4	0-4:24.3.0.255	7
M-Bus Master Disconnect control object 1	0-1:24.4.0.255	70
M-Bus Master Disconnect control object 2	0-2:24.4.0.255	70
M-Bus Master Disconnect control object 3	0-3:24.4.0.255	70
M-Bus Master Disconnect control object 4	0-4:24.4.0.255	70
M-Bus Disconnect control scheduler	0-1:15.0.1.255	22
M-Bus Disconnector script table	0-1:10.0.106.255	9
Event Objects - M-Bus Master Control logs 1	0-1:96.11.4.255	1
Event Objects - M-Bus Master Control logs 2	0-2:96.11.4.255	1
Event Objects - M-Bus Master Control logs 3	0-3:96.11.4.255	1
Event Objects - M-Bus Master Control logs 4	0-4:96.11.4.255	1
M-Bus Master Control log object 1	0-1:24.5.0.255	7
M-Bus Master Control log object 2	0-2:24.5.0.255	7

M-Bus Master Control log object 3	0-3:24.5.0.255	7
M-Bus Master Control log object 4	0-4:24.5.0.255	7
Event Object - M-Bus Event Log	0-0:96.11.3.255	1
M-Bus Event Log	0-0:99.98.3.255	7

Table 13: Extension M IDIS objects

7.2.5 Optional objects

Optional objects according to IDIS P2-OBJ Ed.2.0. may be added by the IDIS device manufacturer. They must be tested as described in sect. 4.

Conformance testing of optional objects and attributes:

- Optional objects/attributes the manufacturer wants to be considered in the IDIS conformance test must be declared explicitly. By doing so optional objects are tested with the same rigor as mandatory objects and the same acceptance criteria apply as for mandatory objects.
- If no optional objects/attributes are declared only the mandatory objects/attributes will be tested and will appear on the test report. The set of mandatory objects/attributes is sufficient to get the test label according to sect. 4.

7.3 Handling Events

A lot of events are generated by the meter itself or by its environment. All these events are logged in several event logs. Additionally they are also used to set and clear errors as well as to trigger alarms.

7.3.1 Events

The event identifiers are defined in IDIS P2-OBJ ed2.0 a copy of which can be found in section 10.

7.3.2 Alarms

Some of the events can trigger alarms. If one of these events occurs, the corresponding flag in the alarm registers is set and an alarm is then raised via communication channel. All alarm flags in the alarm registers remain active until the alarm registers are cleared.

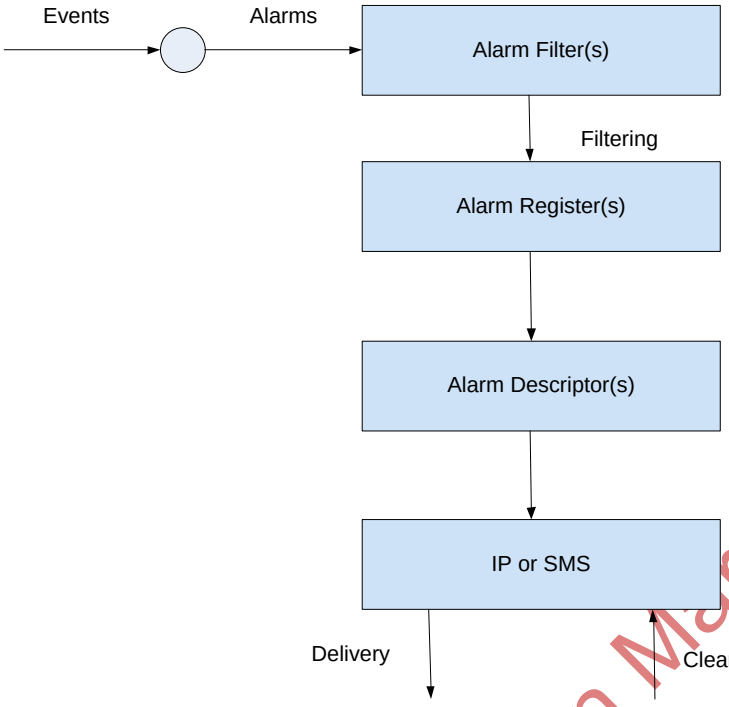


Figure 8 Alarm reporting

Each bit in the alarm registers represents a different alarm. If the bit is set (logical 1) the alarm (corresponding to position of the set bit) was recorded. The value in the **Alarm Registers** is a summary of all active and inactive alarms at that time.

Depending on the capabilities of the HES and the policy of the utility, not all possible alarms are wanted. Therefore the **Alarm Filters** can be programmed to mask out unwanted alarms. The structure of the filter is the same as the structure of the **Alarm Registers**. To mask out unwanted alarms the corresponding bits in **Alarm Filters** should be set to logical 0.

7.3.2.1 Alarming Process

Figure 8 shows the different entities involved in the alarming process.

7.3.2.1.1 Alarm Registers (AR)

- All information on the “cause of the alarm” of the meter is contained in the Alarm Registers.
- Specific bits of Alarm Registers may be internally reset if the “cause of the alarm” has disappeared (e.g. bit1 (battery replace) if the battery has been exchanged). Alternatively, all bits may be externally reset by the client by executing a SET =0 service to the Alarm Registers attribute value (e.g. bit 13 (Fraud attempt) can only be externally reset). In the latter case those bits for which the “cause of alarm” still exists will be set to 1 again and an alarm will be issued.

7.3.2.1.2 Alarm Descriptors (AD)

- The Alarm Descriptors have exactly the same structure as the Alarm Registers. Whenever a bit in the Alarm Registers changes from 0 to 1, then the corresponding bit of the Alarm Descriptors (AD) is set to 1. Resetting the Alarm Registers does not affect the Alarm Descriptors. The set bits of the AD must be reset explicitly by the HES.

7.3.2.1.3 Alarming Process

- The Alarm Descriptors are sent to the HES using the Data-Notification service triggered by the corresponding Alarm Monitor. In IDIS package 2 the Alarm Monitor Threshold value is set to zero. Therefore the Alarm Monitor action is invoked when any of the bits in the Alarm Descriptors value changes from 0 to 1.
- In order to acknowledge the reception of the Alarm the HES has to reset the Alarm Descriptors by invoking the SET=”with bits set to 1 which need to be cleared” on the Alarm Descriptors value. Upon reception of this SET service, the meter clears the corresponding bits in the Alarm Descriptors.
- In order to re-enable the alarm reporting process the HES must reset the reported bits in the Alarm Register. This can only be done by setting all the bits of the Alarm Registers to 0 using the SET service. Prior to this action the HES must read the latest value of the Alarm Register.

Example “Fraud attempt”:
A “fraud attempt” event occurs, setting bit 13 of the Alarm Register to 1. The meter copies the Alarm Register contents into the Alarm Descriptor. If bit 13 was not set in the Alarm Descriptor before then the meter sends the Alarm Descriptor attribute value to the HES using the Data-Notification service via IP (or SMS, depending on the configuration of the “Push Setup - on Alarm" instance). The HES acknowledges the alarm by setting bit13 in the Alarm Descriptor to 1. The meter clears bit 13 in the Alarm Descriptor.
As long as the HES does not clear the bit 13 in the Alarm Register the meter does not send any more alarms on fraud (bit 13 of the Alarm Register cannot change from 0 to 1 and therefore bit 13 in the Alarm Descriptor will not be set). The HES therefore first reads the Alarm Register by applying the GET service and then resets the Alarm Register by applying the SET (AR:=0) service.

Abstract examples:

step	Alarm Register (AR)	Alarm Descriptor (AD)	Meter→ HES communication	Meter ← HES communication
0	0000...	0000...		
1	**1**000...	**1**000...	**Data-Notification**(AD:=1000…) →	
2	1000...	0000...		← SET Request (AD:=1000…)
3	1000...	0000...		← GET Request(AR)
4	1000...	0000...	GET Response (AR:=1000…) →	
5	0000...	0000...		← SET Request (AR:=0)
6	**1**000...	**1**000...	**Data-Notification** (AD:=1000…) →	
7	1**1**00...	1**1**00...	**Data-Notification** (AD:=1100…) →	
8	1100...	0100...		← SET Request (AD:=1000…)
9	11**1**0...	01**1**0...	**Data-Notification** (AD:=0110…) →	
10	1110...	0110...		← GET Request (AR)
11	1110...	0110...	GET Response (AR:=1110…) →	
12	1110...	0000...		← SET Request (AD:=0110…)
13	111**1**...	000**1**...	**Data-Notification** (AD:=0001…) →	
14	0000...	0001...		← SET Request (AR:=0)
15	0000...	0000...		← SET Request (AD:=0001…)

7.3.2.2 COSEM Objects supporting Alarms

Instance Name	OBIS	IC
Alarm Register 1 (class_id 1)	0-0:97.98.0.255	1
Alarm Register 2 (class_id 1)	0-0:97.98.1.255	1
Alarm Filter 1 (class_id 1)	0-0:97.98.10.255	1
Alarm Filter 2 (class_id 1)	0-0:97.98.11.255	1
Alarm Descriptor 1 (class_id 1)	0-0:97.98.20.255	1
Alarm Descriptor 2 (class_id 1)	0-0:97.98.21.255	1
Alarm monitor 1	0-0:16.1.0.255	21
Alarm monitor 2	0-0:16.1.1.255	21

7.3.2.3 Assignment of Alarm Register 1 bits

Alarm Register		
Bit	**Alarm**	**Triggering event**
0	Clock invalid	6
1	Battery replace	7
2	Reserved for future use	-
3	Reserved for future use	-
4	Reserved for future use	-
5	Reserved for future use	-
6	Reserved for future use	-
7	Reserved for future use	-
8	Program memory error	12
9	RAM error	13
10	NV memory error	14
11	Measurement system error	16
12	Watchdog error	15
13	Fraud attempt	40, 42, 44, 46, 49, 50[11]
14	Reserved for future use	-
15	Reserved for future use	-

[11] Any of the listed events shall trigger the alarm.

16	M-Bus communication error ch1	100
17	M-Bus communication error ch2	110
18	M-Bus communication error ch3	120
19	M-Bus communication error ch4	130
20	M-Bus fraud attempt ch1	103
21	M-Bus fraud attempt ch2	113
22	M-Bus fraud attempt ch3	123
23	M-Bus fraud attempt ch4	133
24	Permanent error M-bus ch1	106
25	Permanent error M-bus ch2	116
26	Permanent error M-bus ch3	126
27	Permanent error M-bus ch4	136
28	Battery low on M-bus ch1	102
29	Battery low on M-bus ch2	112
30	Battery low on M-bus ch3	122
31	Battery low on M-bus ch4	132

7.3.2.4 Assignment of Alarm Register 2 bits

Alarm Register		
Bit	**Alarm**	**Triggering event**
0	Total Power Failure	01
1	Power Resume	02
2	Voltage Missing Phase L1	82
3	Voltage Missing Phase L2	83
4	Voltage Missing Phase L3	84
5	Voltage Normal Phase L1	85
6	Voltage Normal Phase L2	86
7	Voltage Normal Phase L3	87
8	Missing Neutral	89
9	Phase Asymmetry	90
10	Current Reversal	91
11	Wrong Phase Sequence	88
12	Unexpected Consumption	52
13	Key Exchanged	48
14	Bad Voltage Quality L1	92

15	Bad Voltage Quality L2	93
16	Bad Voltage Quality L3	94
17	External Alert	20
18	Local communication attempt	53
19	New M-Bus Device Installed Ch1	105
20	New M-Bus Device Installed Ch2	115
21	New M-Bus Device Installed Ch3	125
22	New M-Bus Device Installed Ch4	135
23	Reserved for future use	-
24	Reserved for future use	-
25	Reserved for future use	-
26	Reserved for future use	-
27	M-Bus valve alarm Ch1	164
28	M-Bus valve alarm Ch2	174
29	M-Bus valve alarm Ch3	184
30	M-Bus valve alarm Ch4	194
31	Disconnect/Reconnect Failure	68

7.3.2.4.1 Voltage Level Monitoring based on EN50160

For quality assessment purposes there is also a possibility to monitor the voltage level more in detail.

The meter shall monitor the voltage levels of each phase as an average over a 10 minute interval ($U_{Lx\ average}$). The voltage level is classified according to the following table:

Condition	voltage level
During each period of one week 95 % of $U_{Lx\ average}$ shall be within the range of U_N +/- 10 %; and all $U_{Lx\ average}$ shall be within the range of U_N as defined in EN50160	U_{Lx} NORMAL
Else	U_{Lx} BAD

The corresponding event codes can be found in sect. 10.

7.4 Load Profiles

Different profiles are available in the IDIS meters:

- Load Profiles for electricity metering (Load profile 1, Load profile 2)
- M-Bus Master load profiles (multi utility profiles)

- Billing profile for general metering

Depending on the type of capturing, two main types of profiles are distinguished:

- Synchronous Profiles:
  which are triggered only on a regular basis at the end of the capture period (Load profile 1, Load profile 2 and M-Bus Master load profiles). Special events (e.g. power outages) do not affect the capturing directly but may lead to special entries in the profile status.
- Asynchronous Profiles:
  which are triggered on events (asynchronous profiles).

The billing profile (Billing profile for general metering) is a special case because it can be triggered on a regular basis by a scheduler (synchronously) and/or asynchronously by events.

7.5 Synchronous Load Profiles

7.5.1 Structure

All synchronous profiles share the same structure. It is possible to store the time of the capture (time stamp), the status of several internal events and a selectable number of values, i.e. registers. An example is shown in Table 14

Clock (0-0:1.0.0)	Status	Register 1	Register 2	...
2007-08-12 / 01:00:00	08	1234567	1233567	…
2007-08-12 / 02:00:00	08	1234579	1233584	…
2007-08-12 / 03:00:00	08	1234586	1233598	…
…	…	…	…	…

Table 14 Profile structure representation

7.5.2 Sort Order

The sort order is based on the Profile generic attribute sort_method definition (comp.DLMS UA 1000-1 Ed. 12.0). For IDIS meters sort methods 1 (unsorted fifo) and 4 (sorted by smallest) are supported.

7.5.2.1 Sorted

In IDIS package 2 the buffer entries are sorted according to the attribute time of the Clock object which is always the first object in the list of capture_objects. For IDIS meters using sort method 4 the stored entries are sorted according to the smallest entry (oldest first) of the first column containing the Clock object. Every new entry is stored at the appropriate position in the buffer. If the buffer is full the oldest entry is deleted and the new entry is stored at the appropriate position.

7.5.2.2 Unsorted

If the profile is unsorted, it works as a “first in first out” buffer (it is hence sorted by capturing, and not necessarily by the time maintained in the Clock object). The entries are stored in the same order as they are captured, i.e. most recently captured entry is stored last. When reading the profile, the entries are provided in the same order, i.e. the oldest entry first.

7.5.3 Reset

The buffer of the profiles in the IDIS meters may be cleared by executing the specific method "reset". The execution of the method "reset" triggers the entry '*profiles erased*" in the standard event log (comp. 6.10). The buffer is automatically reset by the meter upon any modification of the attribute capture_period and/or of any modification of the attribute capture_objects.

7.5.4 Capture period

The captured period is controlled by the internal clock and it is synchronized with the internal time, starting always on the full hour (e.g. capture periods of 15 minutes starting at 10:00, 10:15, 10:30, 10:45, 11:00, 11:15 etc.). Only one entry per capture period is captured at the end of the period; i.e. events never generate additional entries in the buffer of the profile. Information on events is recorded in the Profile Status Register and in the Standard Event Log.

The capture period can be selected between **0, 300, 600, 900, 1800, 3600 or 86400 seconds**. If the capture period is set to 0 then the regular capturing is stopped and an external source (e.g. communication, script table, MDI reset) must be used to trigger the capturing of profile entries.

The capture period of 86400 seconds is a special case, it represents daily capturing at midnight. The values are captured once per day at midnight (local time).

7.5.5 Timestamp

The time stamp contains the value of the internal clock at the end of the capture period (local time, type: date_time (octet-string[12]).

7.5.6 Access to the stored values

The stored values of the profile can be retrieved by applying the appropriate xDLMS services to the attribute "buffer". It is possible to read either the entire profile buffer or to use a selective access by range (access selector 1) and/or by entry (access selector 2) as defined in IDIS P2-OBJ Ed.2.0. In IDIS package 2 the support of access by range is mandatory, the access by entry is optional.

7.5.6.1 Normal Read

Every row in the table below shows how the profile should look like when read out. A 'from…to' readout (selective access) request will return a response containing the buffer entries within the 'from…to' range (including the values at the boundaries of the range)

The example below (comp. Table 15) shows the result of a readout request from 13.8.2004 00:00 to 13.8.2004 04:00 for an hourly profile. It is assumed that a power down event - shorter than the capture period – occurred between 03:00 and 04:00.

Date / Time	Status						Register_1	Register_N
	PDN	CAD	DST	DNV	CIV	ERR		
2004-08-13 / 00:00:00	0	0	0	0	0	0	2052	115
2004-08-13 / 01:00:00	0	0	0	0	0	0	2070	115
2004-08-13 / 02:00:00	0	0	0	0	0	0	2098	115
2004-08-13 / 03:00:00	0	0	0	0	0	0	2112	117
2004-08-13 / 04:00:00	1	0	0	0	0	0	2116	119

Table 15 Normal readout

7.5.6.2 Compressed Read

In order to reduce the amount of transmitted data an IDIS meter may support “compressed” readout of the profile buffer (according to DLMS UA 1000-1 Ed. 12.0) the value of a captured object may be replaced by “null-data” if it can be unambiguously recovered from the previous value). In particular, the “null-data” replacement is used:

- for register values: if the value of the buffer entry is same as the value of the previous entry transmitted in the same response sequence.
- for status: the status value is same as the value of the previous entry transmitted in the same response sequence.
- for clock: if date_time(k) = (date_time(k-1) + capture period) within the same response sequence.

7.5.6.2.1 Example for time “compression”

In a synchronous profile the captured time is always increased by the capture period. Therefore, in synchronous profiles the captured time may be “compressed”. In this case, where the second and the following timestamps can be deducted from the previous time stamps, only the first entry is shown with a timestamp. All others entries of the timestamp are replaced by “null-data”.

The example in Table 16 shows the result of a readout request from 13.8.2004 00:00:00 to 13.8.2004 04:00:00 for a hourly profile

Date / Time	Status						Register_1	Register_N
	PDN	CAD	DST	DNV	CIV	ERR		
2004-08-13 / 00:00:00	0	0	0	0	0	0	2052	115
{}	0	0	0	0	0	0	2070	115
{}	0	0	0	0	0	0	2098	115
{}	0	0	0	0	0	0	2112	117
{}	1	0	0	0	0	0	2116	119

Table 16 Compressed readout – Time compressed

{} - *null data (comp.* DLMS UA 1000-2 Ed. 8.0:2014*)*

7.5.6.2.2 Example for time and status ”compression”

Typically the status of the profile remains constant over many capturing periods. In these cases the status may be compressed by replacing the repeated status information by “null-data”.

The example in Table 17 shows the result of a readout request from 13.8.2004 00:00:00 to 13.8.2004 03:00:00 for a hourly profile using time and status compression.

Date / Time	Status						Register_1	Register_N
	PDN	CAD	DST	DNV	CIV	ERR		
2004-08-13 / 00:00:00	0	0	0	0	0	0	2052	115
{}	{}						2070	115
{}	{}						2098	115
{}	{}						2112	117
{}	1	0	0	0	0	0	2116	119

Table 17 Compressed readout – Time and status compressed

7.5.6.2.3 Example for time status and register value compression

Some register values may also remain constant between different capturing periods. In these cases the register values may be compressed by replacing the repeated register value by “null-data”.

The example in Table 18 shows the result of a readout request from 13.8.2004 00:00:00 to 13.8.2004 03:00:00 for a hourly profile using time, status and value compression for Register N.

Date / Time	Status						Register_1	Register_N
	PDN	CAD	DST	DNV	CIV	ERR		
2004-08-13 / 00:00:00	0	0	0	0	0	0	2052	115
{}	{}						2070	{}
{}	{}						2098	{}
{}	{}						2112	117
{}	1	0	0	0	0	0	2116	119

Table 18: Compressed readout – General

7.5.6.3 Compact Array

The compact array is not in the scope of IDIS Package 2.

7.5.6.4 Selective access

To read only a part of the profile buffer selective access either by range (access selector 1) or by entry (access selector 2) may be used (DLMS UA 1000-1 Ed. 12.0). IDIS devices compliant to Package 2 are supporting at least selective access by range.

7.5.7 Profile Status Register

This status register can be captured to show additional information concerning the stored entry. With this information, the HES or MDC may decide whether the captured registers can be used for billing or not. The value of the status register is stored for every entry. The value of the status register of all profiles has a size of 1 byte. The status information is encoded into the 8 bits as shown in Table 19.

Flag	Description
Bit 7 PDN	**Power down**: This bit is set to indicate that a total power outage has been detected during the affected capture period.
Bit 6	**Reserved**: The reserved bit is always set to 0.
Bit 5 CAD	**Clock adjusted**: The bit is set when the clock has been adjusted by more than the synchronization limit.
Bit 4	**Reserved:** The reserved bit is always set to 0.
Bit 3 DST	**Daylight saving**: Indicates whether or not the daylight saving time is currently active. The bit is set if the daylight saving time is active (summer) and cleared during normal time (winter).
Bit 2 DNV	**Data not valid**: Indicates that the current entry may not be used for billing purposes without further validation because a special event has occurred. [12]
Bit 1 CIV	**Clock invalid:** The power reserve of the calendar clock has been exhausted. The time is declared as invalid. At the same time the DNV bit is set.
Bit 0 ERR	**Critical error**: A serious error such as a hardware failure or a checksum error has occurred. If the ERR bit is set then also the DNV bit is set.

Table 19 Load profile status – bit assignment

7.5.8 Events

The following section describes the behavior of the profile and the setting of the status bits considering different events.

In the examples the following colors are used:

entry captured at the end of period when no special events occurred during the capturing period
entry captured at the end of period when one or more special events occurred during the capturing period

The capture period used in all examples is 60 minutes.

7.5.8.1 Season Change

The activation or deactivation of the daylight saving time does not create any additional entries in the buffer. The timestamp together with the DST bit contains enough information to clearly identify when the season change occurred and if the buffer data was captured when daylight saving time was active or not.

7.5.8.2 Power Down

The following section describes the behavior of the profile and the setting of the status bits considering different power down events. A “Power Down” event starts with the complete loss of power in all connected phases and ends with the restoration of the power in at least one of the connected phases.

[12] In cases where the DNV bit is set in the profile status the captured data needs additional validation in the HES

7.5.8.2.1 Power Down within one capture period

The Power Down event affects only one specific capture period. The affected capture period will be marked with Power Down (PDN) bit in the profile status at the end of the capturing period.

Figure 9 and Table 20 show a power down event (from 21:15 to 21:19) within the capture period of 21:00 to 22:00. The entry at 22:00 will be marked with the PDN flag. Since a power down doesn't affect the validity of billing data, the DNV flag is not set.

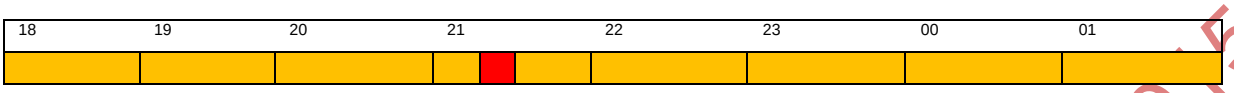


Figure 9 Power failure within capture period

Date / Time	Status bits				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 20:00:00	0	0	0	0	2052	115
2004-08-12 / 21:00:00	0	0	0	0	2070	115
2004-08-12 / 22:00:00	1	0	0	0	2098	115
2004-08-12 / 23:00:00	0	0	0	0	2167	117
2004-08-13 / 00:00:00	0	0	0	0	2180	118

Table 20 Power Down event within a single capture period

7.5.8.2.2 Power Down across several capture periods

Figure 10 and Table 21 show a power down event (from 01:15 to 04:52) affecting all capture periods between 01:00 and 05:00. For the capture periods which completely fall into the power down event (03:00, 04:00) no entry is registered in the load profile buffer.

Figure 10 Power failure within capture period(s)

Date / Time	Status bits				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-13 / 00:00:00	0	0	0	0	2180	118
2004-08-13 / 01:00:00	0	0	0	0	2201	118
2004-08-13 / 02:00:00	1	0	0	0	2205	119
2004-08-13 / 05:00:00	1	0	0	0	2224	121
2004-08-13 / 06:00:00	0	0	0	0	2252	121

Table 21 Power Down event across several capture periods

7.5.8.2.3 Power Down over a season change

Since there are no additional entries generated with a season change power down events over a season change are treated similar to 7.5.8.2.1 and 7.5.8.2.2.

7.5.8.2.4 Exhaust of power reserve

Table 22 shows the situation when a long power down event leads to a discharged power reserve - and therefore to an invalid clock. The power down event starts on 12.8.2004 / 21:15 and ends on

30.08.2004 / 08:45. The power-down is too long to keep the real time clock running with the super cap, the power reserve is exhausted. After power up (30.08./ 08:45), profile entries continue with the time set to the first capture time after the power down (12.08. / 22:00) – with the PDN=1, DNV=1 and CIV=1. Capturing continues using the invalid clock and keeping CIV=1 and DNV=1 until the clock is set.

Date / Time	Internal Clock	
…	…	
30.08. / 08:45	12.08. / 22:00	power resume
30.08. / 09:45	12.08. / 23:00	
30.08. / 10:45	12.08. / 24:00	
30.08. / 11:45	13.08. / 01:00	
…		

Assuming 3 hours and 50 min after power up the clock is set to 30.8.2004 / 12:35, the next regular entry will take place at 30.8.2004 / 13:00. Since the entry does not represent a full capture period the CAD flag will be set to 1.

Date / Time	Internal Clock	
…	…	
30.08. / 12:35	30.08. / 12:35	clock set
30.08. / 13:00	30.08. / 13:00	
…		

The entry at 13.8.2004 / 2:00 is stored as if time was advanced over the end of the next period i.e. CAD and DNV are set to 1. Additionally due to the fact power reserve is exhausted also CIV is set to 1.

Date / Time	Status bits				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 20:00:00	0	0	0	0	2052	115
2004-08-12 / 21:00:00	0	0	0	0	2070	115
2004-08-12 / 22:00:00	1	0	1	1	2125	116
2004-08-12 / 23:00:00	0	0	1	1	2167	117
2004-08-13 / 00:00:00	0	0	1	1	2180	118
2004-08-13 / 01:00:00	0	0	1	1	2201	118
2004-08-13 / 02:00:00	0	1	1	1	2202	119
2004-08-30 / 13:00:00	0	1	0	0	2206	120
2004-08-30 / 14:00:00	0	0	0	0	2257	120
2004-08-30 / 15:00:00	0	0	0	0	2274	121
2004-08-30 / 16:00:00	0	0	0	0	2352	121

Table 22 Exhaust of power reserve – late clock adjustment

If the time adjustment occurs before the end of the 1st capture period after a power-up, the generated entries are additionally marked with the PDN flag.

Remark: due to the exhaust of the power reserve the internal clock stops running and loses its time. At the time of the power up the clock restarts. At the next capture time (12.08. / 22:00) the CIV bit is set to 1.

In the example of Table 23 the clock is set to 30.8.2008 / 08:45 just after power-up (12.08.2008 / 21:15). Therefore the entry at 12.08.2008 / 22:00 is closed and marked with PDN set to 1 due to the fact power down was detected in this period (at 21:15), CIV and DNV set to 1 since the clock is - due to exhaust of power reserve - not running correctly. In addition the CAD is set to 1 since shortly after the power up the time was adjusted. At the next capture time (30.08. / 09:00) the incomplete registration period is marked with PDN=0, CAD=1, DNV=0, CIV=0.

Date / Time	Status bits				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2008-08-12 / 20:00:00	0	0	0	0	2052	115
2008-08-12 / 21:00:00	0	0	0	0	2070	115
2008-08-12 / 22:00:00	1	1	1	1	2071	116
2008-08-30 / 09:00:00	0	1	0	0	2106	118
2008-08-30 / 10:00:00	0	0	0	0	2157	120
2008-08-30 / 11:00:00	0	0	0	0	2174	121

Table 23 Exhaust of power reserve – immediate clock adjustment

7.5.8.3 Setting Time

Clock adjustment larger than a defined synchronization limit is recorded in the event profile and the affected entries in the load profile are marked with the CAD flag.

7.5.8.3.1 Time changes within capture period

Figure 11 and Table 24 show a clock adjustment from 21:15 to 21:20. The entry at 22:00:00 will be marked with the CAD flag.

Figure 11 Forward clock synchronization within capture period

Date / Time	Status bits				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 20:00:00	0	0	0	0	2052	115
2004-08-12 / 21:00:00	0	0	0	0	2070	115
2004-08-12 / 22:00:00	0	1	0	0	2098	115
2004-08-13 / 23:00:00	0	0	0	0	2167	117
2004-08-13 / 00:00:00	0	0	0	0	2180	118

Table 24 Time changes within capture period

Any clock adjustment (forward or backwards) within the capture period is marked in this way.
If the clock adjustment is smaller than the synchronization limit (depending on parameter setting) no entry is recorded.

7.5.8.3.2 Advancing the time over the end of the period

Figure 12 and Table 25 show a clock adjustment from 21:15:37 to 22:22:00. At 22:00:00 an entry is generated with the CAD flag set since the period was not closed correctly. The entry at 23:00:00 is marked with the CAD flag..

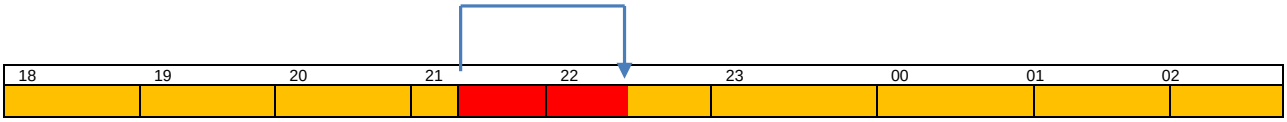


Figure 12 Forward clock synchronization across two consecutive capture periods

Date / Time	Status bits				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 20:00:00	0	0	0	0	2052	115
2004-08-12 / 21:00:00	0	0	0	0	2070	115
2004-08-12 / 22:00:00	0	1	0	0	2075	116
2004-08-12 / 23:00:00	0	1	0	0	2167	117
2004-08-13 / 00:00:00	0	0	0	0	2180	118
2004-08-13 / 01:00:00	0	0	0	0	2201	118

Table 25 Advancing the time over the end of the period

7.5.8.3.3 Advancing the time over several periods

Figure 13 and Table 26 show a clock adjustment from 21:15 to 00:22 of the next day. All generated intermediate values are marked with the CAD flag.

Figure 13 Forward clock synchronization across more consecutive capture periods

Date / Time	Status				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 20:00:00	0	0	0	0	2052	115
2004-08-12 / 21:00:00	0	0	0	0	2070	115
2004-08-12 / 22:00:00	0	1	0	0	2075	116
2004-08-13 / 01:00:00	0	1	0	0	2080	117
2004-08-13 / 02:00:00	0	0	0	0	2090	118
2004-08-13 / 03:00:00	0	0	0	0	2101	118

Table 26 Advancing the time over several periods

7.5.8.3.4 Advancing the time over a season change

No additional recordings are generated. The profile acts the same way as with advancing the clock over one or more periods.

7.5.8.3.5 Setting the time back - sorted

Due to the fact that the profile is sorted, in case of a time change backwards the new entry will be stored at the appropriate position in the buffer.

Figure 14 and Table 27 show a profile after a clock adjustment backwards from 23:15 to 18:42.

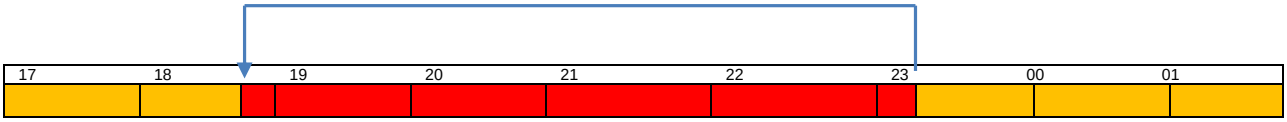


Figure 14 Setting the time back across several capture periods

Before the time change:

Date / Time	Status				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 16:00:00	0	0	0	0	2041	109
2004-08-12 / 17:00:00	0	0	0	0	2047	109
2004-08-12 / 18:00:00	0	0	0	0	2052	110
2004-08-12 / 19:00:00	0	0	0	0	2125	117
2004-08-12 / 20:00:00	0	0	0	0	2201	120
2004-08-12 / 21:00:00	0	0	0	0	2206	120
2004-08-12 / 22:00:00	0	0	0	0	2220	121
2004-08-12 / 23:00:00	0	0	0	0	2257	122

Table 27 Profile before setting the time back

After the time change backwards to 18:42:

The next regular entry is created at 19:00, marked with the CAD flag. If an entry with the same time stamp already exists then the old entry will be overwritten (comp. Table 28).

Date / Time	Status				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 16:00:00	0	0	0	0	2041	109
2004-08-12 / 17:00:00	0	0	0	0	2047	109
2004-08-12 / 18:00:00	0	0	0	0	2052	110
2004-08-12 / 19:00:00	0	1	0	0	2260	123

Table 28 Profile after setting the time back

7.5.8.3.6 Setting the time back - unsorted

In case of an unsorted profile all profile entries remain in the buffer which will lead to duplicated entries.

Table 29 shows a profile before and after (Table 30) a time change backwards from 23:15 to 18:42.

Before the time change:

Date / Time	Status				Register_1	Register_2
	PDN	CAD	DNV	CIV		

2004-08-12 / 16:00:00	0	0	0	0	2041	109
2004-08-12 / 17:00:00	0	0	0	0	2047	109
2004-08-12 / 18:00:00	0	0	0	0	2052	110
2004-08-12 / 19:00:00	0	0	0	0	2125	117
2004-08-12 / 20:00:00	0	0	0	0	2201	120
2004-08-12 / 21:00:00	0	0	0	0	2206	120
2004-08-12 / 22:00:00	0	0	0	0	2220	121
2004-08-12 / 23:00:00	0	0	0	0	2257	122

Table 29 Setting the time back – before

After the time change backwards to 18:42:

All entries between 19:00 and 23:00 are remaining in the buffer after the time change. The next regular entry is marked with the CAD flag.

Date / Time	Status				Register_1	Register_2
	PDN	CAD	DNV	CIV		
2004-08-12 / 16:00:00	0	0	0	0	2041	109
2004-08-12 / 17:00:00	0	0	0	0	2047	109
2004-08-12 / 18:00:00	0	0	0	0	2052	110
2004-08-12 / 19:00:00	0	0	0	0	2125	117
2004-08-12 / 20:00:00	0	0	0	0	2201	120
2004-08-12 / 21:00:00	0	0	0	0	2206	120
2004-08-12 / 22:00:00	0	0	0	0	2220	121
2004-08-12 / 23:00:00	0	0	0	0	2257	122
2004-08-13 / 00:00:00	0	1	0	0	2258	122
2004-08-12 / 19:00:00	0	1	0	0	2260	123

Table 30 Setting the time back – after

Note there are two entries with the same date and time but different values of Register_1 and Register_2 in table above.

7.5.8.4 Profile Reset

If the reset method is executed explicitly or implicitly (as a consequence of a modification in the data structure of the profile, comp DLMS UA 1000-1 Ed. 12.0. the first entry after the reset will contain a valid registration period (considering the modified data structure, if the reset was the consequence of a modification).Table 31 shows the first entry after a reset at 15:45:35.

Date / Time	Status				Register_1	Register_2
	PDN	CAD	DNV	CIV		
12.8.2004 / 16:00:00	0	0	0	0	2041	109

Table 31 Profile Reset

7.6 Billing profile for general metering

The billing profile differs from the other profiles by the way data capturing is performed. For the billing profile implicit periodic capturing is disabled by setting the capture period to zero.

In the billing profile the capturing of the data is managed by the combination of a single-action schedule and a predefined script table “MDI reset / end of billing period”. In addition, asynchronous capturing is possible via explicit local or remote triggering. The collected data is stamped with the time instance when the actual capturing is triggered.

7.6.1 Power down

7.6.1.1 Power failure across capture periods

The regular billing intervals are defined by the date and time definitions specified in the execute_time attribute of a single action schedule. When the time of the internal clock reaches the time instance specified in the single action schedule the capture method of the profile is invoked via the corresponding script defined in the “MDI reset/end of billing period” script table.

In the examples bellow is assumed that the single action schedule is configured to trigger a capturing event every first day of the month at 00:00 (FFFFFF01FF, 00000000).

Figure 15 and Table 32 show a power down from 29.2.2012 23:25 until 1.3.2012 2:15. The buffer values with the time stamp 2012-03-01 / 00:00:00 contain the register values at the time of the power down (29.2.2012, 23:25).

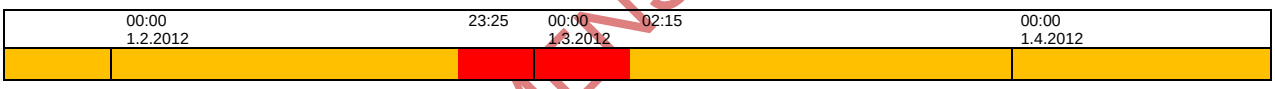


Figure 15 Power failure across billing interval(s)

Date / Time	Register_1	Register_2
2012-02-1 / 00:00:00	2180	115
2012-03-1 / 00:00:00	2201	118
2012-04-1 / 00:00:00	2252	121

Table 32 Power failure across billing interval(s)

7.6.2 Setting Time

7.6.2.1 Advancing the time over the end of the billing interval

Figure 16 and Table 33 show the effects of a clock advancement from 29.2.2012 23:25 to 1.3.2012 2:15.

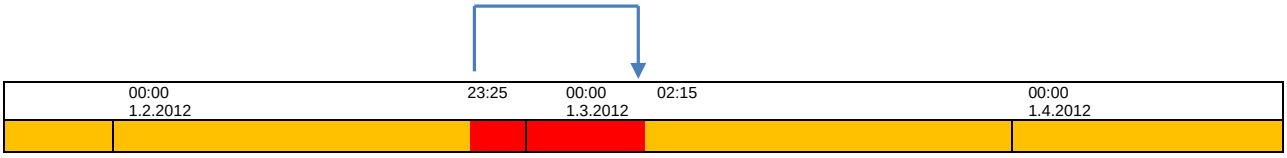


Figure 16 Advancing time over billing interval(s)

Date / Time	Register_1	Register_2
2012-02-1 / 00:00:00	2180	115
2012-03-1 / 00:00:00	2201	118
2012-04-1 / 00:00:00	2252	121

Table 33 Advancing time over billing interval(s)

The buffer values with the time stamp 2012-03-01 / 00:00:00 contain the register values at the time of the clock advancement (29.2.2012, 23:25).

7.6.2.2 Setting the time back over the start of billing interval

Figure 17 and Table 34 show the effects of a clock retarding from 1.3.2012 2:15 to 29.2.2012 23:25.

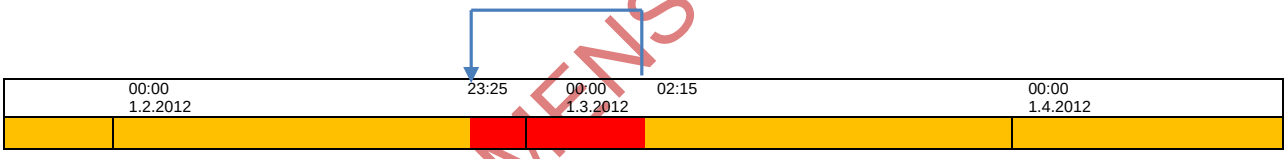


Figure 17 Setting the time back over the start of billing interval

Date / Time	Register_1	Register_2
2012-02-1 / 00:00:00	2180	90
2012-03-1 / 00:00:00	2201	118
2012-04-1 / 00:00:00	2223	121
2012-03-1 / 00:00:00	2231	124
2012-04-1 / 00:00:00	2252	143

Table 34: Setting the time back over the start of billing interval

The buffer values with the first time stamp 2012-03-01 / 00:00:00 contain the register values at the time 2012-03-01 / 00:00:00 *before the clock retarding*.

The buffer values with the first time stamp 2012-04-01 / 00:00:00 contain the register values *at the time of the clock retarding* (01.03.2012, 02:15).

The buffer values with the second time stamp 2012-03-01 / 00:00:00 contain the register values at the time 2012-03-01 / 00:00:00 *after the clock retarding*.

The buffer values with the second time stamp 2012-04-01 / 00:00:00 contain the register values at the time 2012-04-01 / 00:00:00 *after the clock retarding*.

7.6.2.3 Asynchronous billing period reset/end

Data may be captured asynchronously by explicit triggering:
e.g. by pressing the local reset button or by remote invocation of the execute method of the “MDI reset/end of billing period” script. The registered data is stamped with the time instance of the execution of the triggering.

Figure 18 and Table 35 show a billing profile in case when asynchronous triggers are combined with regular triggers
.

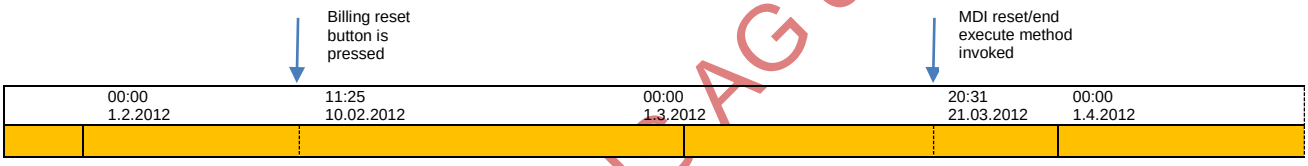


Figure 18 Asynchronous triggering between regular trigger intervals

Date / Time	Register_1	Register_2
2012-02-1 / 00:00:00	2180	90
2012-02-10 / 11:25:00	2201	118
2012-03-1 / 00:00:00	2223	121
2012-03-21 / 00:00:00	2238	124
2012-04-1 / 00:00:00	2252	143

Table 35 Asynchronous billings

7.7 Reading profiles with parameterized access “from”-“to”

The following specifications are valid for any IDIS object which is an instantiation of the interface class “Profile Generic” (e.g. profiles, logs, …).

7.7.1 Interval boundaries

If the requested interval boundaries (“from”, “to”) match the time stamps of profile entries, then the response contains the buffer entries *including the boundaries* of the requested interval.

7.7.2 Covering the DST switchover interval with partly defined time parameters

The “from” and “to” parameters of the requested buffer interval may contain partly defined time stamps according to Table 4. In particular, the Deviation and the Clock Status may be defined or may be left undefined:

case	Deviation	Clock Status
A	0x8000 (not specified)	DST undefined: 0xFF
B	0x8000 (not specified)	DST defined: 0x80/0x00
C	Deviation of the “requested” local time to UTC	DST not active: 0x00

The *DST forward switching* interval (e.g. switching from 02:00 to 03:00) causes only missing profile entries and can therefore be treated according to the rules of a normal readout.

The *DST backwards switching* interval (e.g. switching from 03:00 to 02:00) causes double entries in the profile. If the boundary of a selective readout falls into this switchover period (02:00 before switching to 03:00 after switching) the timestamp of the boundary must include information on the Deviation (case C) or on the Clock Status (case B) in order to uniquely define the time instance.

For *case A* the following rule applies:
The meter treats this request the same way a case B after filling in the DST bit in the “from” and/or “to” time stamp which falls into the DST backwards switching interval (including the boundaries). The filled in DST bit corresponds to the status of the meter’s DST bit at the point of receiving the request.

Examples:
The following examples illustrate cases during the backwards switching interval (before switching: summer time, after switching winter time) from 02:00 to 03:00 (i.e. the profile buffer contains two time intervals with time stamps 02:00 to 03:00). Further, it is assumed that that the registration period is 15 min.

Example 1A:
requesting at 02:17 summer time a reading from (02:14, 0x8000, 0xFF) to (02:16, 0x8000,0xFF) returns the entry for 02:15 summer time.

Example 2A:
requesting at 02:17 winter time a reading from (02:14, 0x8000,0xFF) to (02:16, 0x8000,0xFF) returns the entry for 02:15 winter time.

Example 3A:
requesting at 02:17 winter time a reading from (01:59, 0x8000,0xFF) to (02:16, 0x8000,0xFF) returns all the entries between 02:00 summer time and 02:15 winter time.

Example 1B:
requesting anytime a reading from (02:14, 0x8000,0x80) to (02:16, 0x8000,0x80) returns the entry for 02:15 summer time.

Example 2B:
requesting anytime a reading from (02:14, 0x8000,0x00) to (02:16, 0x8000,0x00) returns the entry for 02:15 winter time.

Example 3B:
requesting anytime a reading from (01:59, 0x8000,0x80) to (02:16, 0x8000,0x00) returns all the entries between 02:00 summer time and 02:15 winter time.

In the following examples we assume DST offset= 60min , time zone= -60min

Example 1C:
requesting anytime a reading from (02:14, 0xFF88,0x00) to (02:16, 0xFF88,0x00) returns the entry for 02:15 summer time.

Example 2C:
requesting anytime a reading from (02:14, 0xFFC4,0x00) to (02:16, 0xFFC4,0x00) returns the entry for 02:15 winter time.

Example 3C:
requesting anytime a reading from (01:59, 0xFF88,0x00) to (02:16, 0xFFC4,0x00) returns all the entries between 02:00 summer time and 02:15 winter time.

7.8 PUSH operation

IDIS package 2 supports PUSH operation triggered:

- on connectivity
- on alarm,
- on installation,
- scheduled.

Push triggered on “power down” is optional and – if available - must be declared for conformance testing.

There are several occasions on which DLMS messages may be ‘pushed’, i.e. sent to the HES without being explicitly requested, e.g.

- at a scheduled time;
- if a monitor threshold is exceeded (e.g. alarm monitor);
- triggered by the HES (wake-up);
- triggered by an event (e.g. power-up/down, key).

Each trigger can cause a message to be sent to a dedicated destination. Therefore for every trigger an individual configuration object is available defining the content and the destination of a push message as well as the medium used:

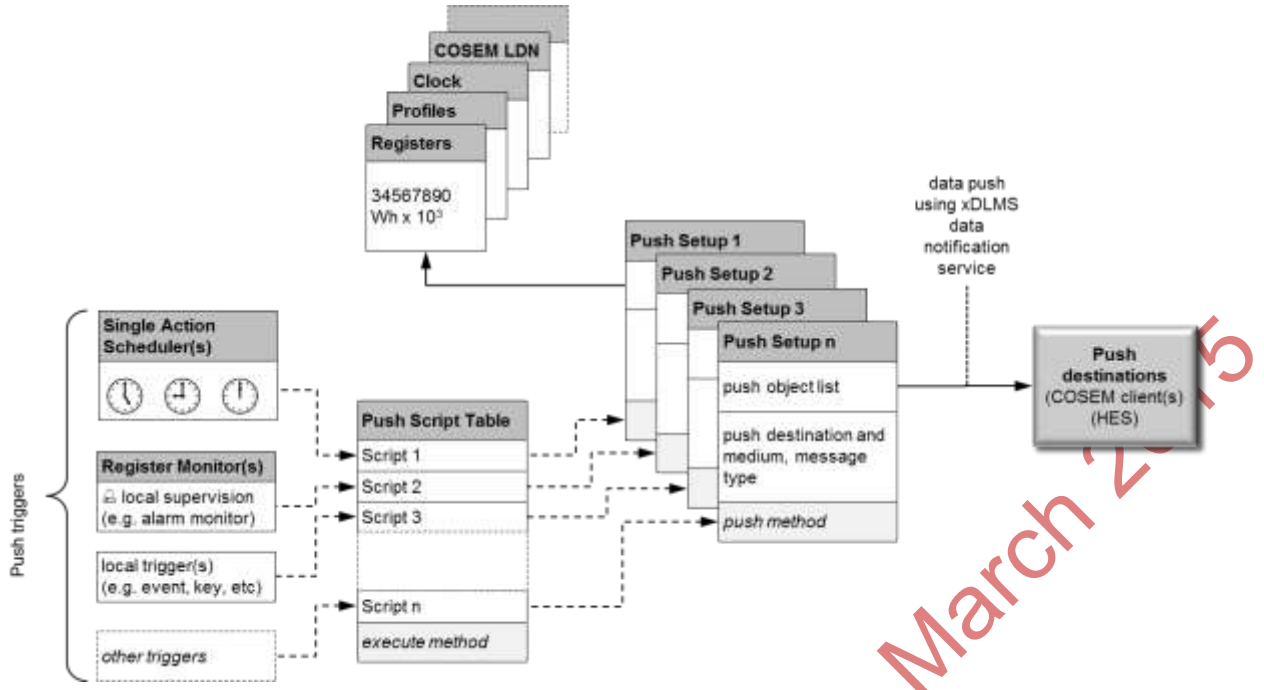


Figure 19 – Interface classes for modeling the push operation

According to Figure 19, the core element is a the “Push setup” interface class which mainly contains a list of references of the object (attributes) to be pushed as well as the push destination and the communication medium to be used. The various triggers (e.g. schedulers, monitors, wake-up call, etc.) call a script entry in a push script table object (new instance of existing script table) which then invokes the push method of the related “Push setup” object. This method at the end handles the sending of the push data to the COSEM client (HES) using the communication channel defined. The “Push setup” interface class also defines the communication time windows and the handling of retries for a push operation.

The "Push setup” interface class contains a list of references to COSEM object attributes to be pushed, as well as the push destination and the communication medium to be used. It also defines the communication time windows (comp. Figure 20) and the handling of retries for a push operation. Please note that the initial trigger comes from somewhere else (e.g. from a scheduler, a monitor, a dedicated event, etc.).

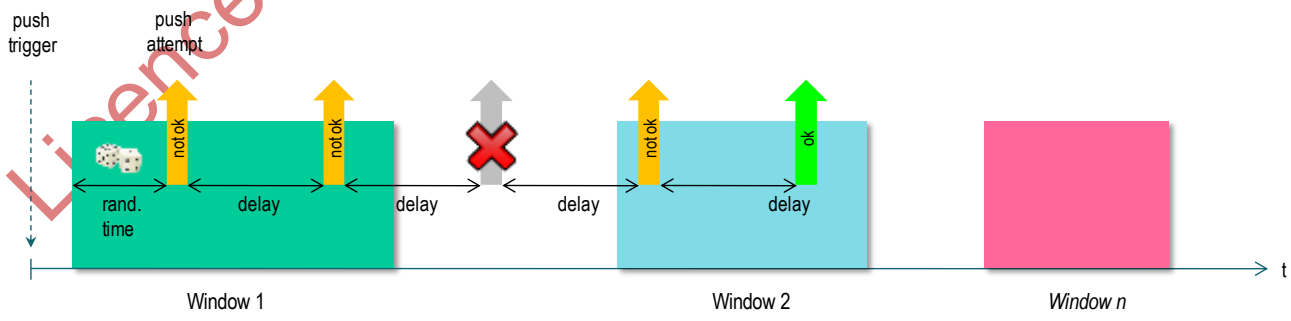


Figure 20 – Push windows and delays

After the push operation has been triggered, the push is executed according to the settings made in the “Push setup” class. Depending on the communication settings the push is executed immediately or as soon as a communication window becomes active. If the push was not successful, retries may be performed.

To send the push data from meter to the HES a new set of unsolicited, non-client/server type unconfirmed services have been defined (DLMS UA 1000-2 Ed. 8.0:2014). These services are used by the server (meter), upon an occurrence of an event, to inform the client (HES) of the value of one or more attributes, as though they had been requested by the client. The push data references are defined in the push_object_list attribute of the "Push setup" object instance. The push service offers a container to transport the resulting data either as a whole or block wise.

All information necessary to further process the data must be part of the application layer data or is predefined in the HES. In case of missing data a null-data-element needs to be sent instead of the actual attribute value.
The push process takes place in a pre-established association context. Depending on the security attributes ciphered or unciphered services are used. For IDIS package 2 the following SAP assignments are used:

Client SAP: 102 (Pre-established Client)
Server SAP: 001 (Management logical device)

Client SAP: 103 (CIP Client)
Server SAP: 001 (Management logical device)

With a push communication only a one-way communication link is established between the meter and the HES.

8. E-Meter Communication

8.1 IDIS Client and Server Architecture

The IDIS Server consists of one COSEM Logical Device (LD name: 0-0:42.0.0.255, SAP: 001) which supports a Pre-established Client (SAP: 102), a Public Client (SAP: 016), and a Management Client (SAP: 001) as illustrated in Figure 21. Details on the use of the different clients can be found in section 8.2.2.

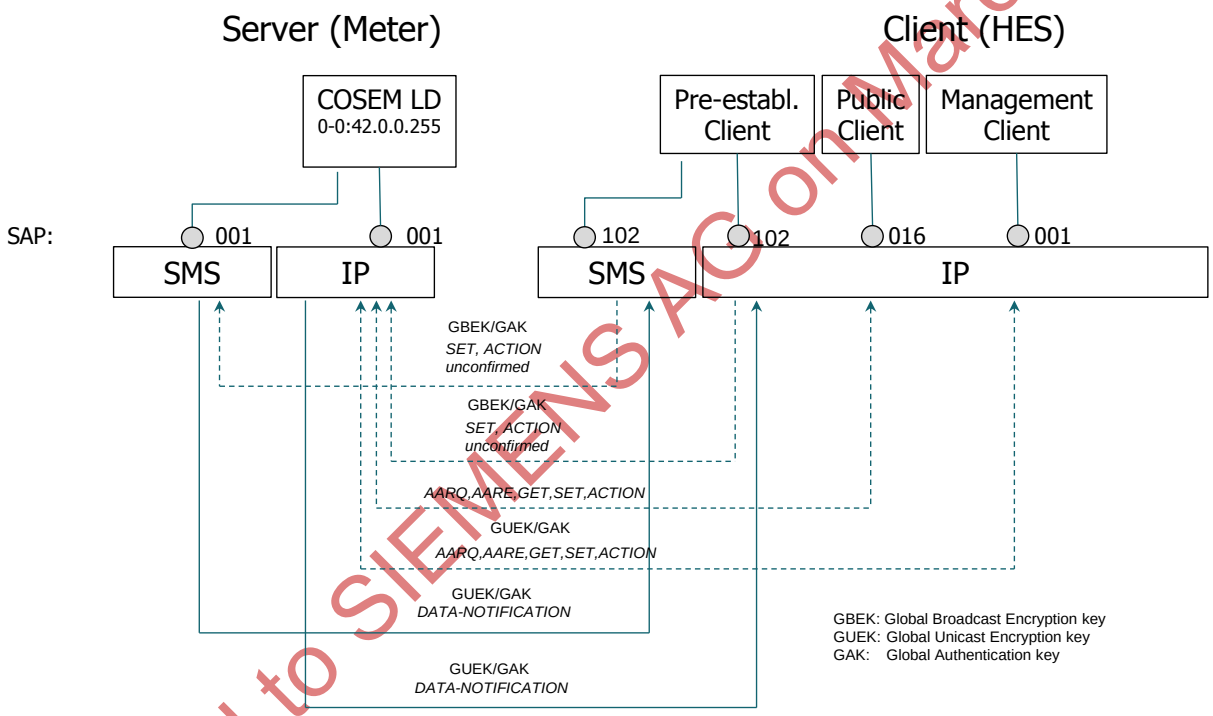


Figure 21 IDIS Client and Server model

The following restrictions apply for the SMS channel:

- Only unconfirmed services can be used.
- The SMS channel can only be used from/to the Pre-established client at HES side.
- In direction to the meter the Broadcast Key must be used (if required by the security policy).
- In direction to the HES the Global Unicast Key must be used (if required by the security policy).

8.2 Application Layer

The E-Meter communicates with the upper system (via I3) using the IEC 62056-53 COSEM Application Layer with extension documented in DLMS UA 1000-2 Ed. 8.0:2014.

8.2.1 Minimal set of services

Logical name services are supported. The Conformance Block (IEC 62056-5-3:2013 Amd.1 CDV) defines the minimal set of supported application layer services:

- General-protection (1)
- General-block-transfer (2)
- Block-transfer-with-get (11)
- Block-transfer-with-set (12)
- Multiple-references (14)
- Data-Notification (16)
- Get (19)
- Set (20)
- Selective-access (21)
- Action (23)

For the multiple references services, a minimum of 16 references must be supported by the GET Request service. For the Set and Action service, the minimum is limited to one.

NB1: Regardless of the limitations above, the GET Request apdu must not be larger than the max apdu size.

NB2: If the data-notification service needs to be protected and/or needs block-transfer, then the general-glo-ciphering [219] service and/or the general-block-transfer [224] service are used for this purpose.

NB3: For the Get and the Set and Action services the IDIS meter must support the specific protection services: glo-get-request, glo-get-response, glo-set-request, glo-set-response, glo-action-request, glo-action-response. Alternatively, the general-glo-ciphering service must be supported.

NB4: For the Get and Set services the IDIS meter must support the block-transfer mode. Alternatively, the general-block-transfer service must be supported.

8.2.1.1 The Invoke-Id-And-Priority byte

is handled according to DLMS UA 1000-2 Ed. 8.0:2014. In particular, Bit 6 (service_class) must be set by the HES in order to get an answer from the meter. The meter only answers if Bit 6 is set in the request.

In the response sent from the meter Bit 6 (service _class) and Bit 7 (Priority) are irrelevant for the HES. The meter must return the Invoke-Id_And-Priority byte as received from the HES.

Remark:
According to DLMS UA 1000-2 Ed. 8.0:2014, p 307 IDIS is using the type **Unsigned8** for the Invoke-Id-And-Priority parameter.

8.2.1.2 Data-Notification

The service Data-Notification (tag nr [15]) is used with:

Long-Invoke-Id-And-Priority configured as follows:

Bit 0-23 (invoke-id-zero …)	unsigned 24 bit (LSB bit 23) number incremented with each invocation of the Data-Notification service
Bit 28 (self-descriptive)	is set to 0,
Bit 29 (processing-option)	is set to 0,
Bit 30 (service_class)	is set to 0,
Bit 31 (priority)	is set to 0,

8.2.2 Minimal set of Associations

At least the following (comp. Table 36) 3 Associations must be supported:

Client	Client L_SAP	Use Cases	Behavior	mandatory Services supported by a Server
Public client	016	• Reading basic device configuration information (e.g. SAP, COSEM logical device name, association, serial nrs, ...)	• Accessible via remote communication and via local interface. • No security; i.e. the COSEM client may access the meter with: LOWEST SECURITY (Logical_Name_Referencing _NoCiphering, Security policy 0, COSEM_lowest_level_security_mechanism_name(0)), independent of the value of the attribute security_policy of object “security setup”. • Get service only to a limited set of attributes • Must be established by the	• Block-transfer-with-get • Get

Client	Client L_SAP	Use Cases	Behavior	mandatory Services supported by a Server
			client using the AARQ service • Closing HDLC (optical): on explicit closure, on timeout, on power-down, or on release request. • Closing remote communication: on explicit closure, on power-down, or on inactivity_ time_out (comp. TCP/UDP setup object) or on release request.	
Management Client	001	1. Management of the device 2. Retrieving data 3. Authorized actions in the meter	• Mandatory on remote communication and on local port • Supports basic communication from the HES to the meter • Must be established by the client using the AARQ service • HLS (backup LLS) • Closing HDLC (optical): on explicit closure, on timeout, on power-down, or on release request. • Closing remote communication: on explicit closure, on inactivity_ time_out (comp. TCP/UDP setup object) or on release request.	• Block-transfer-with-get • Block-transfer-with-set • Get • Set • Multiple-references • Selective Access • Action • General-block-transfer • General-protection
Pre established client	102	4. All unconfirmed application layer services e.g.: Broadcasting time, image transfer, TOU tables, load control (scheduled	• Not available on local port • Client suited to support broadcast with encryption and authentication (application context must be completely defined)	• Set • Action • Data-Notification • General-block-transfer • General-protection

Client	Client L_SAP	Use Cases	Behavior	mandatory Services supported by a Server
		or spontaneous)	• Mandatory on remote communication • No LLS, no HLS • Always established (triggered by power-up) • Limited set of access services to a limited set of objects	

Table 36 Minimal set of supported associations

The list of COSEM objects in IDIS P2-OBJ Ed.2.0 explicitly assigns clients and access rights to all attributes used in IDIS package 2.

Access Security is supported by High Level Security and Low Level Security.

Message Security is supported using security suite id 0 (AES-GCM-128)

8.2.2.1 Enciphering of the InitiateRequest field in the RLRQ and AARQ pdus

Context name Security policy	Logical_Name_Referencing_No_Ciphering =0	Logical_Name_Referencing_With_Ciphering =0	Logical_Name_Referencing_No_Ciphering >0	Logical_Name_Referencing_With_Ciphering >0
RLRQ	No InitiateRequest Unciphered InitiateRequest	Ciphered InitiateRequest	Not possible	Ciphered InitiateRequest
AARQ	Unciphered InitiateRequest	Ciphered InitiateRequest	Not possible	Ciphered InitiateRequest

In case security policy >0:

An AARQ carrying non ciphered context information (context_id different from Logical_Name_Referencing_With_Ciphering) must be rejected by the server with an “error action” according to Table 37.

8.2.2.2 Power-down

For the remote comm. port:

- The context for the pre-established client is automatically re-established upon power up.
- For G3-PLC communication:

The context of the management client established before the power-down is automatically re-established upon power up; i.e. a power-down will not close the association of the management client.

- For other communication media:
  A power-down will automatically close the association of the management client.

For the local (optical) port:

- A power-down will automatically close any association on the local port.

8.2.2.3 Pre-established Association

Used by the pre-established client.

The pre-established application shares the security concept with the management client. The application context is implicitly defined as:

- max receive pdu_size= 1224[13]
- max send pdu size= 1224
- DLMS version nr= 6
- Quality of service= not used
- Ciphering info= not used
- Conformance= SET, ACTION, DATA-NOTIFICATION, GENERAL-BLOCK-TRANSFER, GENERAL-PROTECTION
- Application context name= Logical_Name_Referencing_With_Ciphering
- Security setup reference= 0-0:43.0.0.255

Due to the fact that there is no explicit application association established, the client can use ciphered application context even if the security policy is set to 0. In such a case the security header of the frame provides the necessary information related to the applied security. Ciphered and unciphered services can be used in this case.

The objects and attributes which are accessible by the pre-established client are defined in IDIS P2-OBJ Ed.2.0.

8.2.2.4 Association Release Request RLRQ

If in the “Association Release Request “service (sent by the client) the optional parameter “user information” is present, then server must answer with the “Association Release Response” service with the parameter “user information” also present.

If in the RLRQ the parameter “user information” is not present then it must also be not present in the RLRE.

[13] IPv6 minimum MTU minus COSEM wrapper overhead

8.2.2.5 Application association object

In IDIS there exists one current association object representing the information on the currently open association.

Current Association (class_id 15)	logical_name: 0-0:40.0.0.255

8.2.2.6 Handling lost Associations

If the server responds to any Get or Set or Action request from the client with an ”ExceptionResponse” due to a lost association then the client has to send an AARQ again (has to establish the association again).

8.2.2.7 Associations on different communication ports

The following rules apply:

- On the local communication port (IEC 62056-21), only one association can be opened at a time.
- On the remote communication port (IP) several associations may be opened at the same time.
- At different communication ports, several associations (with the same client or with different clients) may be opened at the same time.
- If a client wants to use several communication ports at the same time it must open an association at each communication port separately.
- Synchronization of Internal memory access must be handled by the manufacturer.

8.2.3 Error handling in the application layer

The protocol error management copes with situations where the peer station does not act/react in the way normally expected. The following specifications of the error situations and the corresponding error information allow the recipient of the information to react in the appropriate way.

8.2.3.1 General rule

The server always answers to a service request: either with the proper response or with an EXCEPTION response or confirmed service error.

8.2.3.2 Errors related to the AARQ service

If the server receives an AARQ service the following actions (Table 37) are specified in case of an erroneous condition (condition NOT fulfilled)

Condition NOT fulfilled in the AARQ service	Action performed by the server
Server Id = Management logical device	No response
Client Id = public or broadcast or management	No response

Condition NOT fulfilled in the AARQ service	Action performed by the server
Association NOT OPEN	AARE.user_information= Confirmed service error with: initiate-error.initiate.refused-by-the-VDE-Handler Alternatively, Exception response(state-error=service-not-allowed, service-error=operation-not-possible)
Protocol Version = OK	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-provider.no-common-acse-version
Context Name = RECEIVED	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.application-context-not-supported
Context Name = OK[14]	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.application-context-not-supported
(Secured Context AND Calling AP Title = RECEIVED) OR (Not Secured Context)[15]	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentication-required
ACSE Requirement = RECEIVED	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentication-required
ACSE Requirement = OK	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentication-required
Mechanism Name = RECEIVED	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentication-mechanism-required
Mechanism Name = OK	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentication-mechanism-not-recognised
Authentification Value = RECEIVED	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentification-failure
Authentification Value = OK	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.authentification-failure
User Information = RECEIVED	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.no-reason-given
Dedicated-Key = OK	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.no-reason-

[14] All optional fields which are present must be tested and the test must be fulfilled.

[15] The calling AP Title is the system title and it is accepted without any additional checking.

Condition NOT fulfilled in the AARQ service	Action performed by the server
	given AARE.user-information = ConfirmedServiceError.InitiateError.Initiate.other
Proposed-dlms-version = 6	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.no-reason-given AARE.user-information = ConfirmedServiceError.InitiateError.Initiate.dlm-version-too-low
Proposed-Conformance = OK[16]	AARE.result = reject-permanent AARE.result-source-diagnostic = acse-service-user.no-reason-given AARE.user-information = ConfirmedServiceError.InitiateError.Initiate.incompatible-conformance

Table 37 Error events associated to the AARQ service

8.2.3.3 Errors related to the Get/Set/Action services

Errors related to the Get/Set/Action services are shown in Table 38

Condition NOT fulfilled in the service	Action performed by the server
Association opened	Exception response(state-error = service-not-allowed, service-error=service-not-supported)
Get, Set, Action request encryption or authentication OK	Exception response(state-error = service-not-allowed, service-error=operation-not-possible)
Get, Set, Action request tag correct or format is correct	Exception response(state-error =service-not-known, service-error=operation-not-possible)
Get, request with type = next long get and (“Block number received” in GetRequestNext == last block number sent by the server or “Block number received” in GetRequestNext == last block number sent by the server -1) Example: Last block sent by the server: 3 “Block number received”=3 (server will send block 4) or 2 (server will send block 3 again)	Get response (Data-Access-Result = long-get-aborted)
Set, request with type = next long set and	Set response (Data-Access-Result = long-set-aborted)

[16] the value of the conformance block must be the one defined in this specification.

Condition NOT fulfilled in the service	Action performed by the server
("Block number received" in SetRequestNext == last block number sent by the client or "Block number received" in SetRequestNext == last block number sent by the client -1) Example: Last block sent by the client: 3 "Block number received"=3 (client will send block 4) or 2 (client will send block 3 again) (Block number == block expected) or (block number == block expected -1)	
Get, Set response with data block, the service is present in the negotiated conformance block[17]	Get Set response (Data-Access-Result = scope-of-access-violated)
For Set request with data block, the service is present in the negotiated conformance block.	Set response (Data-Access-Result = scope-of-access-violated)
For Get with selective access, the service is present in negotiated conformance block	Get response (Data-Access-Result = scope-of-access-violated)
For any Get, Set or Action request :	
COSEM attribute/method descriptor is correct	Get, Set, Action Response (Data-Access-Error = object-undefined)
The client has the right access right	Get, Set, Action Response (Data-Access-Error = read-write-denied)
For Get, Set, Action request with selective access, access selector is correct	Get, Set, Action Response (Data-Access-Result = scope-of-access-violated)
For Get, Set, Action request with selective access, access parameters are correct	Get, Set, Action Response (Data-Access-Result = scope-of-access-violated)
Set, Action data type Ok	Set, Action Response (Data-Access-Error = type-unmatched)
Set, Action data content Ok	Set, Action Response (Data-Access-Error = other-reason)

Table 38 Error events associated to GET, SET and ACTION

8.2.3.4 Errors related to the Data-Notification service

There are no error messages foreseen.

[17] This case may only occur if the client during conformance negotiation proposes not to support Get or Set and then during operation still uses Get or Set.

8.2.3.5 Errors related to the RLRQ service

Errors related to the RLRQ service are shown in Table 39

Condition NOT fulfilled in the service	Action performed by the server
Association OPEN	RLRE.reason = normal Alternatively, Exception response(state-error=service-not-allowed, service-error=operation-not-possible)
User Information = RECEIVED	RLRE.reason = not_finished

Table 39 Error events associated to the RLRQ service

8.2.3.6 Errors in secured services

The following tables are related to application association when the security policy is higher than 0.

8.2.3.6.1 Errors in the secured AARQ service

Errors in the secured AARQ service are shown in Table 40

Condition NOT fulfilled in the service	Action performed by the server
Secured initiate request	AARE.result = reject-permanent AARE.result-source-diagnostic = no reason given
Received Security Header == authenticated & encrypted	AARE.result = reject-permanent AARE.result-source-diagnostic = no reason given
FC received > FC previous	AARE.result = reject-permanent AARE.result-source-diagnostic == no reason given
Authentication succeeded	AARE.result = reject-permanent AARE.result-source-diagnostic = no reason given
Deciphering succeeded	AARE.result = reject-permanent AARE.result-source-diagnostic = no reason given

Table 40 Error events associated to the secured AARQ service

8.2.3.6.2 Errors in the secured RLRQ service

Errors in the secured RLRQ service are shown in Table 41

Condition NOT fulfilled in the service	Action performed by the server
RLRQ secured	RLRE.reason = not_finished
Received Security Header = authenticated & encrypted	RLRE.reason = not_finished
FC received > FC previous	RLRE.reason = not_finished

Authentication succeeded	RLRE.reason = not_finished
Deciphering succeeded	RLRE.reason = not_finished

Table 41 Error events associated to the secured RLRQ service

8.3 Network Connectivity

The network connectivity of an IDIS meter is controlled by the auto connect objects (see also 11) and the Push setup – On Connectivity:

Instance Name	OBIS	IC
Auto connect	0-0:2.2.1.255	29
Push setup – On Connectivity	0-0:25.9.0.255	40

The following auto connect modes are supported:

- (101) The IDIS meter is permanently connected to the IP network and can be reached by the HES or DC via its known IP address.
- (102) The IDIS meter is permanently connected to the IP network within the validity time of the calling window can be reached by the HES or DC via its known IP address. The device is disconnected outside the calling window. There is no connection possible outside the calling window.
- (103) The IDIS meter is permanently connected to the IP network within the validity time of the calling window and can be reached by the HES or DC via its known IP address. The device is disconnected outside the calling window but it connects to the IP network when the connect method is invoked. If the HES needs to communicate to the meter outside the calling window the HES shall wake-up the meter via SMS or via CSD call
- (104) The IDIS meter is usually disconnected. It connects to the IP network when the connect method is invoked. If the HES needs to communicate to the meter the HES shall wake-up the meter via SMS or via CSD call.

The *Push on Connectivity* is triggered each time a new network connection is established. A new network connection may be caused internally (e.g. reconnection in mode (101) , starting a new connection window in mode (102) and (103) or externally by sending a wake-up signal to the meter in mode (104) or (103).

NB for modes (102) and (103): After completion of the window the connection is maintained as long as communication on application layer occurs. The actual closing of the connection is triggered by the timeout of the lower layer (e.g. TCP timeout).

8.3.1 Wake-Up Process

In conjunction with GPRS (or GSM/PPP) communication the meter may not always be connected to the IP network. In this case the IDIS meter must be set to auto connect mode (104) in the auto connect object. Upon receiving the wake-up call (SMS or CSD) from the HES, the meter verifies if the calling number is listed in the “list_of_allowed_callers” attribute of the “auto answer” object. If the call is of call_type(1) the meter connects immediately to the network.

The meter's IP address may be provided to the HES by the Data-Notification service.

The following additional (in addition to the objects listed in section 8.3) objects are foreseen to support the Wake-Up process:

Instance Name	OBIS	IC
Auto answer	0-0:2.2.0.255	28

The security related issues are treated in 9.1.

8.3.1.1 GPRS or GSM/PPP connection to the IP network

The HES may initiate a connection of the meter to the IP network via a digital connection (e.g. GPRS) or via an analog modem (e.g. GSM/PPP) by choosing the corresponding caller_id. In order to do so the Auto Answer object in the meter must be configured accordingly. In particular, one caller_id must be assigned for call_type(0) (CSD call, resulting in a modem connection) and a different caller_id must be assigned for call_type(1) (call or empty message, resulting in a GPRS connection).

Remark:
If the HES has not two different caller_ids available, the Auto Answer object provides the means of a "workaround" to control the establishment of a modem connection or a GPRS connection. This is done by adding the same caller_id with both call_types into the list_of_allowed_callers (see Note 1 in the Auto Answer class description). In this case the number_of_rings parameter must be set large enough to allow the initiator of the call to control the behavior of the receiver of the call without any knowledge of the time instances of the rings at the receiver's side. **IDIS package 2 does not support this option.**

8.4 Lower layers for IP communication

At minimum one IP channel must be supported. On this channel either the IPv4 or IPv6 protocol may be used; i.e. it is not possible to run a IPv4 and a IPv6 connection on this channel in parallel. The choice between IPv4 and IPv6 is made by setting attribute IP_reference in the TCP-UDP setup object accordingly.

8.4.1 IPv4

The IPv4 channel is configured via the COSEM object "IPv4 setup" (class_id: 42) as defined in IDIS P2-OBJ Ed.2.0.

8.4.2 IPv6

The IPv6 channel is configured via the COSEM object "IPv6 setup" (class_id: 48) as defined in IDIS P2-OBJ Ed.2.0

8.4.3 TCP

The TCP channel is configured via the COSEM object “TCP-UDP setup” (class_id: 41) as defined in IDIS P2-OBJ Ed.2.0. If the TCP connection is closed then the meter also releases the application association.

8.4.4 UDP

The UDP channel is configured via the COSEM object “TCP-UDP setup” (class_id: 41) as defined in IDIS P2-OBJ Ed.2.0. The application association is closed due to inactivity timeout.

8.4.5 Physical channels

8.4.5.1 GSM

IP connection through the GSM channel is configured via the COSEM object “PPP setup” (class_id: 44) as defined in IDIS P2-OBJ Ed.2.0.

8.4.5.2 GPRS/UMTS

The GPRS/UMTS channel is configured via the COSEM object “GPRS setup” (class_id: 45) as defined in IDIS P2-OBJ Ed.2.0.

8.4.5.3 Ethernet

The Ethernet channel is configured via the COSEM object “MAC address setup” (class_id: 43) as defined in IDIS P2-OBJ Ed.2.0.

8.4.5.4 G3-PLC

The G3 channel is configured and managed via the following COSEM objects:

- “G3-PLC MAC setup” (class_id: 91) containing the parameters to setup and manage the MAC layer.
- “G3-PLC MAC layer counters” (class_id: 90) containing statistical information on the packet exchange on MAC layer.
- “G3-PLC 6LoWPAN adaptation layer setup” (class_id: 92) to setup and manage the 6loWPAN adaptation layer.
- MAC address setup” (class_id: 43) as defined in IDIS P2-OBJ Ed.2.0

8.5 SMS as a general communication channel

The SMS channel supports xDLMS services with the following restrictions:

- SMS is used as one-way channel only,
- therefore only unconfirmed services are allowed (from client: SET, ACTION, unconfirmed, to client: Data-Notificaton),

- therefore communication is restricted to/from the Pre-established client only (comp. Figure 21),
- used security key from HES: Global Broadcast Key,
- used security key to HES: Global Unicast Key,
- more details on security can be found in section 9.2.,
- erroneous apdus or confirmed service requests are ignored by the meter without any error message,
- the max pdu size for SMS communication is 138[18],
- no block transfer service is supported with SMS communication.

The xDLMS pdus are transported via the SMS channel by means of the “SMS Short Wrapper” defined in DLMS UA 1000-2 Ed. 8.0:2014. Where IDIS uses for the client the SAP (source and destination) 102 and for the server SAP (source and destination) 001

For PUSH operation: the meter must support the Data-Notification service via the SMS channel.

[18] If liable SMS service for longer messages can be provided the max pdu size may be extended to 1224.

9. E-Meter Security Features

IDIS applies the information security methods described in sect. 9.2 of DLMS UA 1000-2 Ed. 8.0:2014.

In IDIS package 2 the use of dedicated keys is not foreseen; i.e. the HES does not need to support the management of the dedicated keys. However, the meters are equipped with all the necessary features to support dedicated keys.

9.1 Security for Wake-Up

9.1.1 Security for CSD (Circuit Switched Data) call wake-up

Only CSD calls which are explicitly whitelisted in the attribute “list_of_allowed_callers” of the object “Auto Answer” and are of call_type(0) are accepted by the meter. For more details, see DLMS UA 1000-1 Ed. 12.0.

9.1.2 Security for SMS wake-up

Only SMS which are explicitly whitelisted in the attribute “list_of_allowed_callers” of the object “Auto Answer” and are of call_type(1) are accepted by the meter. For more details, see DLMS UA 1000-1 Ed. 12.0.

9.2 Security for SMS as a general communication channel

Only SMS which are explicitly whitelisted in the attribute “list_of_allowed_callers” of the object “Auto answer” and are of call_type(1) are accepted by the meter. For more details, see DLMS UA 1000-1 Ed. 12.0.

9.2.1 Receiving unconfirmed services from HES

- Only possible in pre-established association;
- Depending on the security policy set ***global broadcast encryption and/or global authentication key*** may be used.
- Services: unconfirmed SET and unconfirmed ACTION

9.2.2 Transmitting unconfirmed services to HES

- Only possible in pre-established association
- Depending on the security policy set ***global unicast encryption and/or global authentication key*** may be used.
- Services: General-glo-ciphering [219] with ciphered DATA-NOTIFICATION. In the General-Glo-Services pdu the field system title must always be transmitted.

```
General-Glo-Ciphering ::= SEQUENCE
{
   system-title                          OCTET STRING,
   ciphered-service                      OCTET STRING
}
```

9.3 Security for PUSH/PULL

Security for IDIS package 2 is based on the security definitions of package 1. In addition, package 2 defines the handling of multiple virtual communication channels (see also Figure 21) with only one security setup (see 9.4).

9.3.1 Use of the Frame counters

Depending on the security policy applied the meter uses the Global Unicast Key for all outgoing messages. Therefore the transmit frame counter is incremented for every message sent independently of the channel [19](to “Pre-established Client via SMS”, to “Pre-established Client via IP” or to “Management Client via IP”; see also Figure 21 IDIS Client and Server model) used.

- The HES shall process the frame counter in the received message for each receiving channel (as listed above) individually: For each specific channel the HES validates the received frame counter according to the following rule:
  A message received on a specific channel is discarded if the frame counter in the received message is smaller or equal to the frame counter expected by the receiver on this channel.
- Further, since only unconfirmed services are allowed on channels using the Pre-established Client, for security reasons the HES shall reject any Response service received on these channels; i.e. only the Data notification service is accepted.

On communication media not maintaining the order between transmitted and received message sequences (UDP, SMS) the following rules must be applied at the HES side:

- Prior deciphering the Message sequence is re-ordered according to increasing frame counters.
- *A message is rejected if the frame counter in the received message is smaller or equal to the frame counter in the previously received message for any of the individual channels.*
- Consistency is checked using additional information in the frames (e.g. block counters, invoke-id). Inconsistent frames are rejected.

9.4 Security setup object

The IDIS server may support several security contexts. Each security context is configured by its security setup object.

The “Management Client association” and the “Pre-established Client association” share the same security context. Therefore there is only one security setup object through which this security context is configured:

[19] A specific “Channel” consists of the combination of a specific Client and a specific communication medium

Security Setup (class_id 64)	logical_name: 0-0:43.0.0.255

In this security setup object, the global unicast key is related to the “Management Client association” and to the “Pre-established Client association”. The global broadcast key is related to the “Pre-established Client association” while the authentication key is related to both the “Management Client association” and the “Pre-established Client association”. The attributes “security_policy” and the “security_activate” are the same for both associations.

Table 42 shows the relations between the keys and the association for the security setup object 0-0:43.0.0.255 (for the management and pre-established association).

Security parameter	Valid for management association	Valid for pre-established association	Valid for CIP association
global unicast key	yes	yes	no
global broadcast key	no	yes	no
global authentication key	yes	yes	no
security_policy	yes	yes	no
security_activate	yes	yes	no

Table 42: relation of the security parameters to the associations

The optional “CIP Client association” (comp. 6.11.3) has its own security context. Therefore there is one additional security setup object through which this security context may be configured:

Security Setup (class_id 64)	logical_name: 0-0:43.0.1.255

In this security setup object, the global unicast key is related to the CIP.

Table 43 shows the relations between the keys and the association for the security setup object 0-0:43.0.1.255 (for the CIP client association).

Security parameter	Valid for management association	Valid for pre-established association	Valid for CIP association
global unicast key	no	no	yes
global broadcast key	no	no	yes
global authentication key	no	no	yes
security_policy	no	no	yes
security_activate	no	no	yes

Table 43: relation of the security parameters to the associations

NB:
Since there is only one logical device the meter's system title is always the same for all associations. There is only one master key in the meter and it is used to exchange the keys for all security contexts.

9.4.1 Security Setup

Management Client on remote communication:

- The *client_system_title* is transmitted as part of the AARQ and copied into the COSEM object security setup, attribute: client_system_title.
- From this time instance on the meter uses this *client_system_title* to decipher the pdus from the Management Client.
- After closing the association the attribute *client_system_title* remains in the COSEM object security setup, attribute: client_system_title.

Management Client on local port:

- *client_system_title* is transmitted as part of the AARQ BUT NOT copied into the COSEM object security setup, attribute: client_system_title.
- From this time instance on the meter uses this *client_system_title* to decipher the pdus on the local port.

Pre-established Client on remote communication:

- The *client_system_title* used by the server in the pre-established association is the value stored in the COSEM object security setup, attribute: client_system_title.
- Any of the attributes granted GET access for the Management client (see IDIS P2-OBJ Ed.2.0) may be pushed to the Pre-established client via the Data-Notification service.

CIP Client on local port:

- The *client_system_title* used by the server in the CIP association is the value stored in the CIP COSEM object security setup, attribute: client_system_title.

Public Client on local port:

- *client_system_title* is NOT transmitted as part of the AARQ.

Only the receive Frame Counters are accessible via public client, the security attributes of the security setup object are only accessible via the Management client. In particular, key changes can only be done via the management client.

9.4.2 The use of Global keys and Dedicated keys

The following rules concerning the keys apply:

- At a given point of time there exists one specific set of keys (dedicated[20], global) per security context.
- There exists always a unique master key per device which cannot be changed.
- Dedicated keys are valid during the lifetime of an association; i.e. the dedicated key is generated and taken in use with the opening of the association. The key is destroyed automatically by the server upon closing of the association.
- The lifetime of the Global Key is limited by the range of the dedicated Frame Counters. The global key must be changed explicitly by the client (using the method “global_key_transfer” of the object “Security Setup”). The new global key is encrypted with the master key. The global keys are generated and managed by the HES.
- If a ded_service is requested by the HES but the dedicated key is not known by the meter, then the meter returns an error: exception_response(service-not-allowed, operation-not-possible)

The following rules concerning the frame counters apply:

- Frame Counters used with dedicated keys are independent of the FCs used with global keys.
- Frame Counters used with dedicated keys are handled internally in the meter (no access via COSEM object provided)
- FCs used with dedicated keys are reset (to 0) when a new association is established (new ded key generated by HES – transmitted with InitiateRequest, encrypted with global key)

Note on the use of dedicated keys:

The use of Dedicated Keys in IDIS is optional. Consequently: IDIS meters **must** accept RLRQ and AARQ **without** a Dedicated Key. IDIS meters **may** accept RLRQ and AARQ **with** a Dedicated Key

9.4.3 Frame counters

The following applies for security context shared by the pre-established client and the management client. For the optional security context of the CIP client the frame counter is implicit.

Each IDIS server (meter) must store the following (comp. Table 44) frame counters per security context (GET access via public client):

Key	FC Tx	FC Rx
Broadcast	na	FCRxb
Unicast	FCTxu	FCRxu

Table 44: Frame Counters stored in an IDIS server

[20] Dedicated keys are assigned only during the establishment of the Association

Each time any of the global keys is changed (by using the master key) the corresponding FCRx is reset to 0 (FCRx = 0)

The frame counters can be accessed via public client (IC=1, data):

Security - Receive frame counter - broadcast key (class_id 1) FCRxb	logical_name: 0-0:43.1.1.255
Security - Receive frame counter - unicast key FCRxu	logical_name: 0-0:43.1.0.255

9.4.3.1 Re-synchronizing the FCs

When operating with *global keys* then the HES re-synchronizes its FCs by reading the FCs from the meters (via public client).

When operating with *dedicated keys* the HES re-synchronizes its FCs by first closing the current association (using global unicast keys) and after re-opening the association (using global unicast keys) by changing the dedicated keys (the FCs are automatically reset).

9.4.3.2 In case of local access using security:

Whenever there is local access involving security then the unicast FC (FCRxu) is updated. Due to the local access the HES is not aware of the updating of the FC. In this situation the HES must re-synchronize the FCs as defined in 9.4.3.1.

9.4.4 Application association establishment:

For High level Security the AA establishment is done using the GMAC authentication mechanism (mechanism_id(5)). The association establishment follows the process as described in sect. 9.2.7.4 of DLMS UA 1000-2 Ed. 8.0:2014.

In pass 3 and 4 of the peer authentication process the global unicast encryption key, and the authentication key (if in use) are used. Therefore the attribute “LLS secret” (nr 7) of the current association and the optional method “change_HLS secret” are not relevant.

NOTE: there is only ONE association object; i.e. the “current association” (OBIS: 0.0.40.0.0.255).

9.4.4.1 Default passwords and global keys for interoperability testing

For testing purposes the following (comp. Table 45) default security material should be used:

Security parameter	Default value (hex)
LLS default password	12345678
Global Authentication key	0xD0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF
Global Broadcast key	0x0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00
Global Encryption key	0x00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Global CIP Authentication key	0xC0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF

Global CIP Encryption key	0x10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
Master key	0X00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF

Table 45 Default values of the security parameters for testing

NOTE: For a specific security context, each time any of the global keys is changed (by using the master key) the corresponding FC is reset to 0.

9.4.5 Putting a meter into field

The following process is performed:

1. In the factory, the security policy is set to zero.
2. Commissioning is performed during installation via the local port using HLS (mechanism_id 3 or 4) or LLS (without using any encryption key). In this case it is assumed that the ”HLS secret” is set in the factory into the meter and that the ”HLS secret” is known to the client at the local port.
   Alternatively, HLS (mechanism_id 5) might be used but in this case the default keys (set in the factory) have to be exposed and need therefore to be changed (remotely) after commissioning.
3. Securing the meter: The security policy is set to >0 either locally or remotely after commissioning of the meter.
4. If keys are used in step 2 then they have to be exchanged remotely.

9.4.6 Using Keys

The keys are used as shown in Table 46.

Key	Pre-established Client	Management Client	Public Client	CIP client (optional)
Glo-broadcast The same key is used for all meters under one HES (or DC). Used with unconfirmed services (invoke_id: bit 6 set to 1).	yes	No	No	No
Glo-unicast A unique key for each meter at least under one HES (or DC).	yes	Yes	No	No
Glo-authentication The same key is used for all meters under one HES (or DC).	yes	Yes	No	No
Ded-unicast A unique key for each meter at least under one HES (or DC).	no	yes	No	No
Glo-unicast CIP A unique key for each meter / consumer information portal	No	No	No	Yes
Glo-authentication CIP A unique key for each meter / consumer information portal	No	No	No	Yes

Table 46: Use of the keys

9.4.6.1 Rules to change the Key

- All global keys are changed by using the security_setup.global_key_transfer method. The method is accessible only via the Management Client.

  Possible responses from the meter:

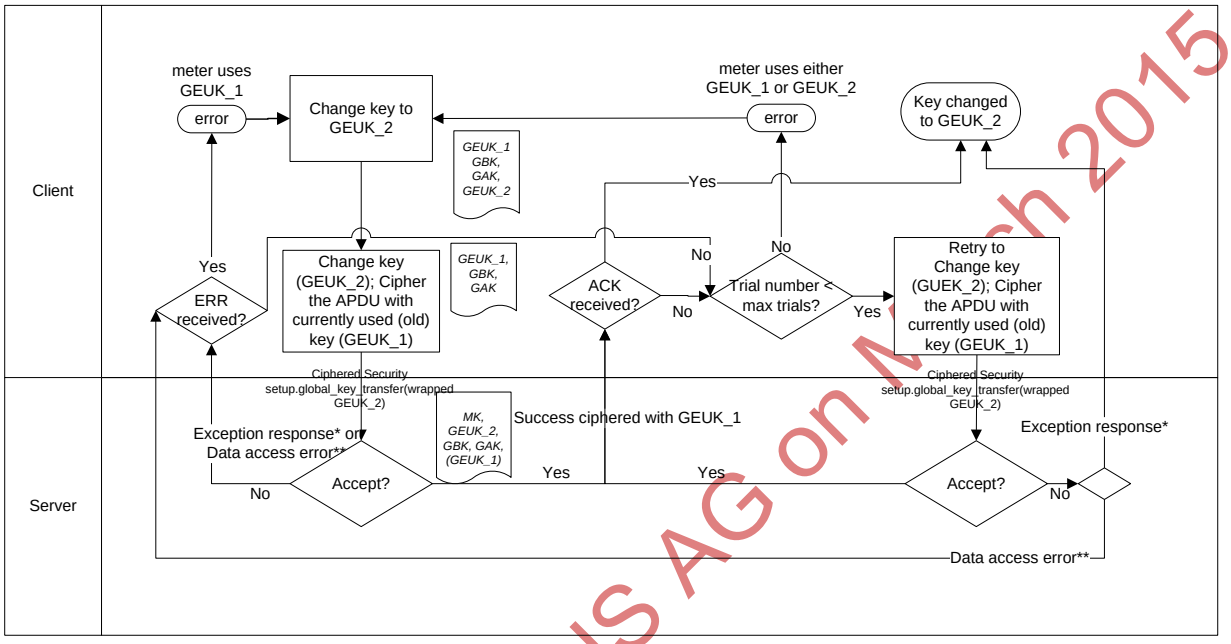
  - If the “new” key is accepted, then the meter sends Action Response(same invoke_id and priority as the request): **SUCCESS** ciphered with “currently used” key. From this point on, meter uses the “new” key (replacing the “currently used” key with “new” key) and resets FC.
  - If the type of the data in the Action Request is not correct then the meter answers with Action Response(same invoke_id and priority as the request): **Data_Access_Error=Type unmatched**.
  - If the meter cannot decrypt the pdu (request encrypted with invalid key) Response(state-error=service-not-allowed, service-error=operation-not-possible).

Figure 22 shows the key exchange process in more details.

In addition, the following applies:

- In case the security policy is different from 0 and if the global unicast key or the authentication key is lost the meter cannot be accessed anymore. The meter must be exchanged .
- If only the Glo-authentication key is changed none of the FCs is reset.

- If the Glo-unicast key is changed then the FC of the Glo-unicast key is reset automatically to 0.
- If the Glo-broadcast key is changed then the FC of the Glo-broadcast key is reset automatically to 0 (LN 0-0:43.1.1.255)



*Unique Exception response (state-error = service-not-allowed, service-error=operation-not-possible) clearly identifying wrong key was used in this situation
**Data access error identifying wrong type or content of data in Action request.

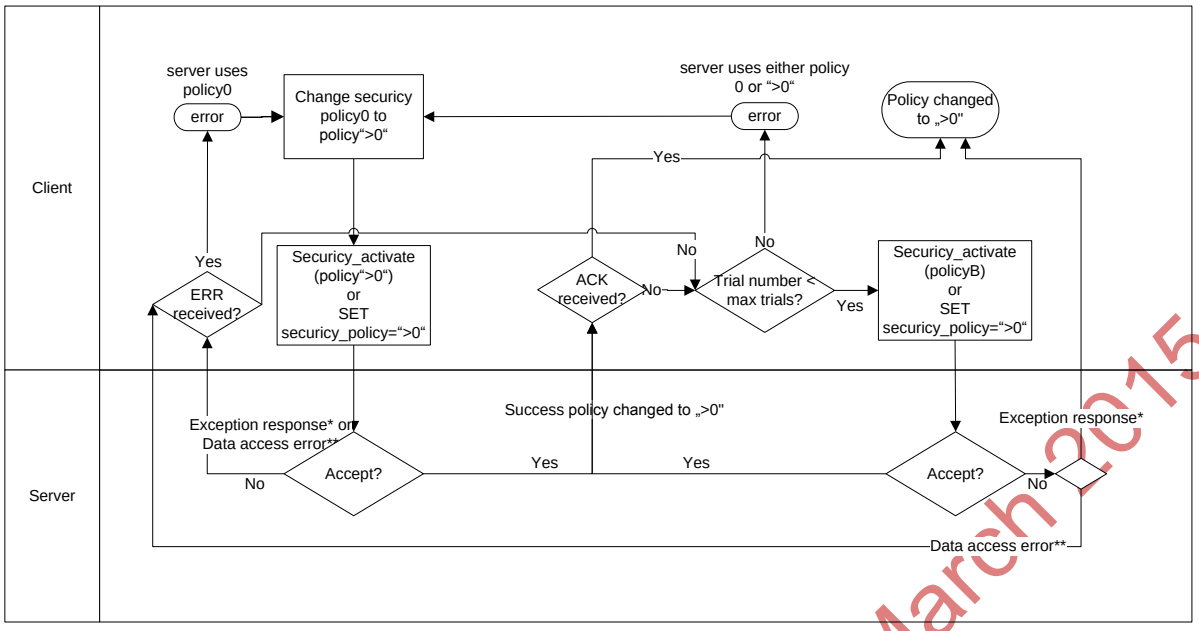
Figure 22 : Changing the Global Key in an IDIS server

9.4.7 Changing the Security Policy

The Security Policy may be changed by invoking the security_activate method of the security setup object, or by setting the security_policy attribute of the security setup object. Only the Management Client can change the security policy, considering the following rules:

Security Policy	apdu
Increase	Unciphered (if starting from security policy = 0) or ciphered
decrease	ciphered only

The sequence diagram for changing the Security Policy is shown in Figure 23.



*Unique Exception response (state-error = service-not-allowed, service-error=operation-not-possible) clearly identifying wrong key was used in this situation
**Data access error identifying wrong type or content of data in Action request.

Figure 23: Changing the Security Policy in an IDIS server

10. Appendix: Event Codes

The following section list the event codes used in package 2. The list is a copy of the corresponding list in IDIS P2-OBJ Ed.2.0.

The support of some event codes is mandatory for the BASIC IDIS functionality, the support of some events is dependent on the implemented IDIS extensions as shown in Table 47.

The following abbreviations apply:

O optional: the IDIS meter does not need to support this event. However if the event is supported then the listed code must be used.
M mandatory for the BASIC functionality
M-G mandatory for GSM/GPRS communication
M-G3 mandatory for G3-PLC communication
M-D mandatory for extension D
M-L mandatory for extension L
M-M mandatory for extension M

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
1	Power Down	Indicates a complete power down of the device. Please note that this is related to the device and not necessarily to the network.	x										M
2	Power Up	Indicates that the device is powered again after a complete power down.	x										M
3	Daylight saving time enabled or disabled	Indicates the regular change from and to daylight saving time. The time stamp shows the time before the change. This event is not set in case of manual clock changes and in case of power failures.	x										M
4	Clock adjusted (old date/time)	Indicates that the clock has been adjusted. The date/time that is stored in the event log is the old date/time before adjusting the clock.	x										M
5	Clock adjusted (new date/time)	Indicates that the clock has been adjusted. The date/time that is stored in the event log is the new date/time after adjusting the clock.	x										M
6	Clock invalid	Indicates that clock may be invalid, i.e. if the power reserve of the clock has exhausted. It is set at power up.	x										M
7	Replace Battery	Indicates that the battery must be exchanged due to the expected end of life time.	x										O
8	Battery voltage low	Indicates that the current battery voltage is low.	x										O
9	TOU activated	Indicates that the passive TOU has been activated.	x										M
10	Error register cleared	Indicates that the error register was cleared.	x										M
11	Alarm register cleared	Indicates that the alarm register was cleared.	x										M
12	Program memory error	Indicates a physical or a logical error in the program memory.	x										M
13	RAM error	Indicates a physical or a logical error in the RAM.	x										M

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
14	NV memory error	Indicates a physical or a logical error in the non volatile memory	x										M
15	Watchdog error	Indicates a watch dog reset or a hardware reset of the microcontroller.	x										M
16	Measurement system error	Indicates a logical or physical error in the measurement system	x										M
17	Firmware ready for activation	Indicates that the new firmware has been successfully downloaded and verified, i.e. it is ready for activation	x										M
18	Firmware activated	Indicates that a new firmware has been activated	x										M
19	Passive TOU programmed	The passive structures of TOU or a new activation date/time were programed	x										O
20	External alert detected	Indicates signal detected on the meter's input terminal	x										O
21	*reserved for future use*												
22	*reserved for future use*												
23	*reserved for future use*												
24	*reserved for future use*												
25	*reserved for future use*												
26	*reserved for future use*												
27	*reserved for future use*												
28	*reserved for future use*												
29	*reserved for future use*												
30	*reserved for future use*												
31	*reserved for future use*												
32	*reserved for future use*												
33	*reserved for future use*												
34	*reserved for future use*												
35	*reserved for future use*												
36	*reserved for future use*												
37	*reserved for future use*												
38	*reserved for future use*												
39	*reserved for future use*												
40	Terminal cover removed	Indicates that the terminal cover has been removed.		x									O
41	Terminal cover closed	Indicates that the terminal cover has been closed.		x									O
42	Strong DC field detected	Indicates that a strong magnetic DC field has been detected.		x									O
43	No strong DC field anymore	Indicates that the strong magnetic DC field has disappeared.		x									O
44	Meter cover removed	Indicates that the meter cover has been removed.		x									O
45	Meter cover closed	Indicates that the meter cover has been closed.		x									O

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
46	Association authentication failure (n time failed authentication)	Indicates that a user tried to gain LLS access with wrong password (intrusion detection) or HLS access challenge processing failed n-times		x									M
47	One or more parameters changed		x										M
48	Global key(s) changed	One or more global keys changed	x										M
49	Decryption or authentication failure (n time failure)	Decryption with currently valid key (global or dedicated) failed to generate a valid APDU or authentication tag		x									M
50	Replay attack	Receive frame counter value less or equal to the last successfully received frame counter in the received APDU Event signalizes as well the situation when the DC has lost the frame counter synchronization.		x									M
51	FW verification failed	Indicates the transferred firmware verification failed i.e. cannot be activated.	x										M
52	Unexpected consumption	Indicates consumption is detected at least on one phase when the disconnector has been disconnected	x										O
53	*Reserved for future use*												
54	*reserved for future use*												
55	*reserved for future use*												
56	*reserved for future use*												
57	*reserved for future use*												
58	*reserved for future use*												
59	Disconnector ready for manual reconnection	Indicates that the disconnector has been set into the Ready_for_reconnection state and can be manually reconnected			x								M-D
60	Manual disconnection	Indicates that the disconnector has been manually disconnected.			x								M-D
61	Manual connection	Indicates that the disconnector has been manually connected.			x								M-D
62	Remote disconnection	Indicates that the disconnector has been remotely disconnected.			x								M-D
63	Remote connection	Indicates that the disconnector has been remotely connected.			x								M-D
64	Local disconnection	Indicates that the disconnector has been locally disconnected (i.e. via the limiter or current supervision monitors).			x								M-D
65	Limiter threshold exceeded	Indicates that the limiter threshold has been exceeded.			x								M-D
66	Limiter threshold ok	Indicates that the monitored value of the limiter dropped below the threshold.			x								M-D
67	Limiter threshold changed	Indicates that the limiter threshold has been changed			x								M-D

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
68	Disconnect/Reconnect failure	Indicates that the a failure of disconnection or reconnection has happened (control state does not match output state)			x								O
69	Local reconnection	Indicates that the disconnector has been locally re-connected (i.e. via the limiter or current supervision monitors).			x								M-D
70	Supervision monitor 1 threshold exceeded	Indicates that the supervision monitor threshold has been exceeded.			x								M-L
71	Supervision monitor 1 threshold ok	Indicates that the monitored value dropped below the threshold.			x								M-L
72	Supervision monitor 2 threshold exceeded	Indicates that the supervision monitor threshold has been exceeded.			x								M-L
73	Supervision monitor 2 threshold ok	Indicates that the monitored value dropped below the threshold.			x								M-L
74	Supervision monitor 3 threshold exceeded	Indicates that the supervision monitor threshold has been exceeded.			x								M-L
75	Supervision monitor 3 threshold ok	Indicates that the monitored value dropped below the threshold.			x								M-L
76	Undervoltage L1	Indicates undervoltage on at least L1 phase was detected.									x		M
77	Undervoltage L2	Indicates undervoltage on at least L2 phase was detected.									x		M
78	Undervoltage L3	Indicates undervoltage on at least L3 phase was detected.									x		M
79	Overvoltage L1	Indicates overvoltage on at least L1 phase was detected.									x		M
80	Overvoltage L2	Indicates overvoltage on at least L2 phase was detected.									x		M
81	Overvoltage L3	Indicates overvoltage on at least L3 phase was detected.									x		M
82	Missing voltage L1	Indicates that the voltage on at least L1 phase has fallen below the Umin threshold for longer than the time delay.									x		M
83	Missing voltage L2	Indicates that the voltage on at least L2 phase has fallen below the Umin threshold for longer than the time delay.									x		M
84	Missing voltage L3	Indicates that the voltage on at least L3 phase has fallen below the Umin threshold for longer than the time delay.									x		M
85	Voltage L1 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.									x		M
86	Voltage L2 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.									x		M
87	Voltage L3 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.									x		M
88	Phase sequence reversal	Indicates wrong mains connection. Usually indicates fraud or wrong installation. For poly phase connection only!	x										O

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
89	Missing neutral	Indicates that the neutral connection from the supplier to the meter is interrupted (but the neutral connection to the load prevails). The phase voltages measured by the meter may differ from their nominal values	x										O
90	Phase Asymmetry	Indicates phase asymmetry due to large unbalance of loads connected									x		O
91	Current Reversal	Indicates unexpected energy export (for devices which are configured for energy import measurement only)		x									O
92	Bad Voltage Quality L1	Indicates that the voltage of L1 does NOT fulfill the following condition: during each period of one week 95 % of the 10 min mean r.m.s, values of the supply voltage are within the range of Un+/- 10 % and all 10 mín mean r.m.s. values of the supply voltage shall be within the range of Un + 10%/-15%. (acc. EN50160:2010, section 4.2.2)									x		O
93	Bad Voltage Quality L2	Indicates that the voltage of L2 does NOT fulfill the following condition: during each period of one week 95 % of the 10 min mean r.m.s, values of the supply voltage are within the range of Un+/- 10 % and all 10 mín mean r.m.s. values of the supply voltage shall be within the range of Un + 10%/-15%. (acc. EN50160:2010, section 4.2.2)									x		O
94	Bad Voltage Quality L3	Indicates that the voltage of L3 does NOT fulfill the following condition: during each period of one week 95 % of the 10 min mean r.m.s, values of the supply voltage are within the range of Un+/- 10 % and all 10 mín mean r.m.s. values of the supply voltage shall be within the range of Un + 10%/-15%. (acc. EN50160:2010, section 4.2.2)									x		O
95	*reserved for future use*												
96	*reserved for future use*												
97	*reserved for future use*												
98	*reserved for future use*												
99	*reserved for future use*												
100	Communication error M-Bus channel 1	Indicates a communication problem when reading the meter connected to channel 1 of the M-Bus				x							M-M
101	Communication ok M-Bus channel 1	Indicates that the communication with the M-Bus meter connected to channel 1 of the M-Bus is ok again.				x							M-M
102	Replace Battery M-Bus channel 1	Indicates that the battery must be exchanged due to the expected end of life time.				x							M-M
103	Fraud attempt M-Bus channel 1	Indicates that a fraud attempt has been registered.				x							M-M
104	Clock adjusted M-Bus channel 1	Indicates that the clock has been adjusted.				x							M-M
105	New M-Bus device installed channel 1	Indicated the meter (M-Bus master) has registered a M-Bus device connected to channel 1 with a new serial number				x							M-M
106	Permanent Error M-Bus	Severe error reported by M-Bus device				x							M-M

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
	channel 1												
107	*reserved for future use*												
108	*reserved for future use*												
109	*reserved for future use*												
110	Communication error M-bus channel 2	Indicates a communication problem when reading the meter connected to channel 2 of the M-Bus				x							M-M
111	Communication ok M-bus channel 2	Indicates that the communication with the M-Bus meter connected to channel 2 of the M-Bus is ok again.				x							M-M
112	Replace Battery M-Bus channel 2	Indicates that the battery must be exchanged due to the expected end of life time.				x							M-M
113	Fraud attempt M-Bus channel 2	Indicates that a fraud attempt has been registered in the M-Bus device.				x							M-M
114	Clock adjusted M-Bus channel 2	Indicates that the clock has been adjusted.				x							M-M
115	New M-Bus device installed channel 2	Indicated the meter (M-Bus master) has registered a M-Bus device connected to channel 2 with a new serial number				x							M-M
116	Permanent Error M-Bus channel 2	Severe error reported by M-Bus device (Bit 3 in MBUS status EN13757)				x							M-M
117	*reserved for future use*												
118	*reserved for future use*												
119	*reserved for future use*												
120	Communication error M-bus channel 3	Indicates a communication problem when reading the meter connected to channel 3 of the M-Bus				x							M-M
121	Communication ok M-bus channel 3	Indicates that the communication with the M-Bus meter connected to channel 3 of the M-Bus is ok again.				x							M-M
122	Replace Battery M-Bus channel 3	Indicates that the battery must be exchanged due to the expected end of life time.				x							M-M
123	Fraud attempt M-Bus channel 3	Indicates that a fraud attempt has been registered.				x							M-M
124	Clock adjusted M-Bus channel 3	Indicates that the clock has been adjusted.				x							M-M
125	New M-Bus device installed channel 3	Indicated the meter (M-Bus master) has registered a M-Bus device connected to channel 3 with a new serial number				x							M-M
126	Permanent Error M-Bus channel 3	Severe error reported by M-Bus device (Bit 3 in MBUS status EN13757)				x							M-M
127	*reserved for future use*												
128	*reserved for future use*												
129	*reserved for future use*												
130	Communication error M-bus channel 4	Indicates a communication problem when reading the meter connected to channel 4 of the M-Bus				x							M-M
131	Communication ok M-bus channel 4	Indicates that the communication with the M-Bus meter connected to channel 4 of the M-Bus is ok again.				x							M-M

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
132	Replace Battery M-Bus channel 4	Indicates that the battery must be exchanged due to the expected end of life time.				x							M-M
133	Fraud attempt M-Bus channel 4	Indicates that a fraud attempt has been registered.				x							M-M
134	Clock adjusted M-Bus channel 4	Indicates that the clock has been adjusted.				x							M-M
135	New M-Bus device installed channel 4	Indicated the meter (M-Bus master) has registered a M-Bus device connected to channel 4 with a new serial number				x							M-M
136	Permanent Error M-Bus channel 4	Severe error reported by M-Bus device (Bit 3 in MBUS status EN13757)				x					-		M-M
137	*reserved for future use*												
138	*reserved for future use*												
139	*reserved for future use*												
140	No connection timeout	There has been no remote communication on application layer for a predefined period of time; i.e. meter could not be reached remotely.										x	O
141	Modem Initialization failure	Modem's response to initialization AT command(s) is invalid or ERROR or no response received										x	M-G
142	SIM Card failure	SIM card is not inserted or is not recognized[21]										x	M-G
143	SIM Card ok	SIM card has been correctly detected[21]										x	M-G
144	GSM registration failure	Modem's registration on GSM network was not successful										x	M-G
145	GPRS registration failure	Modem's registration on GPRS network was not successful										x	M-G
146	PDP context established	PDP context is established										x	M-G
147	PDP context destroyed	PDP context is destroyed										x	M-G
148	PDP context failure	No Valid PDP context(s) retrieved										x	M-G
149	Modem SW reset	Modem restarted by SW reset										x	M-G
150	Modem HW reset	Modem restarted by HW reset (this event is not issued after a general power resume)										x	O
151	GSM outgoing connection	Modem is successfully connected, initiated by an outgoing call.										x	M-G
152	GSM incoming connection	Modem is successfully connected, initiated by an incoming call										x	M-G
153	GSM hang-up	Modem is disconnected										x	M-G
154	Diagnostic failure	Modem's response to diagnostic AT command(s) ("+CPIN?", "+CSQ", "+CREG?", "+CGREG?", "+COPS?", "+CGACT?", "+CPMS?") is invalid or ERROR or no response received.										x	O
155	User initialization failure	Modem's initialization AT command(s) – specified in attribute 3 of the modem configuration object - is invalid. Error message or no response from the modem.										x	M-G

[21] The detection of the SIM card status is supported by the corresponding AT commands as listed in 3GPP TS 27.007

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
156	Signal quality low	Signal strength too low, not known, or not detectable										x	O
157	Auto Answer Number of calls exceeded	Number of calls has exceeded (in mode(1) or mode(2)) the values given in the attribute number_of_calls.										x	M-G
158	Local communication attempt	Indicates a successful communication on any local port has been initiated.										x	O
159	*reserved for future use*												
160	Manual disconnection M-Bus channel 1	Indicates that the disconnector has been manually disconnected.					x						O
161	Manual connection M-Bus channel 1	Indicates that the disconnector has been manually connected.					x						O
162	Remote disconnection M-Bus channel 1	Indicates that the disconnector has been remotely disconnected.					x						M-M
163	Remote connection M-Bus channel 1	Indicates that the disconnector has been remotely connected.					x						M-M
164	Valve alarm M-Bus channel 1	Indicates that a valve alarm has been registered.					x						O
165	Local disconnection M-Bus channel 1	Indicates that the disconnector has been locally disconnected.					x						M-M
166	Local connection M-Bus channel 1	Indicates that the disconnector has been locally connected.					x						M-M
167	*reserved for future use*												
168	*reserved for future use*												
169	*reserved for future use*												
170	Manual disconnection M-Bus channel 2	Indicates that the disconnector has been manually disconnected.						x					O
171	Manual connection M-Bus channel 2	Indicates that the disconnector has been manually connected.						x					O
172	Remote disconnection M-Bus channel 2	Indicates that the disconnector has been remotely disconnected.						x					M-M
173	Remote connection M-Bus channel 2	Indicates that the disconnector has been remotely connected.						x					M-M
174	Valve alarm M-Bus channel 2	Indicates that a valve alarm has been registered.						x					O
175	Local disconnection M-Bus channel 2	Indicates that the disconnector has been locally disconnected.						x					M-M
176	Local connection M-Bus channel 2	Indicates that the disconnector has been locally connected.						x					M-M
177	*reserved for future use*												
178	*reserved for future use*												
179	*reserved for future use*												
180	Manual disconnection M-Bus channel 3	Indicates that the disconnector has been manually disconnected.							x				O
181	Manual connection M-Bus channel 3	Indicates that the disconnector has been manually connected.							x				O

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
182	Remote disconnection M-Bus channel 3	Indicates that the disconnector has been remotely disconnected.							x				M-M
183	Remote connection M-Bus channel 3	Indicates that the disconnector has been remotely connected.							x				M-M
184	Valve alarm M-Bus channel 3	Indicates that a valve alarm has been registered.							x				O
185	Local disconnection M-Bus channel 3	Indicates that the disconnector has been locally disconnected.							x				M-M
186	Local connection M-Bus channel 3	Indicates that the disconnector has been locally connected.							x				M-M
187	*reserved for future use*												
188	*reserved for future use*												
189	*reserved for future use*												
190	Manual disconnection M-Bus channel 4	Indicates that the disconnector has been manually disconnected.								x			O
191	Manual connection M-Bus channel 4	Indicates that the disconnector has been manually connected.								x			O
192	Remote disconnection M-Bus channel 4	Indicates that the disconnector has been remotely disconnected.								x			M-M
193	Remote connection M-Bus channel 4	Indicates that the disconnector has been remotely connected.								x			M-M
194	Valve alarm M-Bus channel 4	Indicates that a valve alarm has been registered.								x			O
195	Local disconnection M-Bus channel 4	Indicates that the disconnector has been locally disconnected.								x			M-M
196	Local connection M-Bus channel 4	Indicates that the disconnector has been locally connected.								x			M-M
197	*reserved for future use*												
198	*reserved for future use*												
199	*reserved for future use*												
200	*manufacturer specific*												
201	*manufacturer specific*												
202	*manufacturer specific*												
203	*manufacturer specific*												
204	*manufacturer specific*												
205	*manufacturer specific*												
206	*manufacturer specific*												
207	*manufacturer specific*												
208	*manufacturer specific*												
209	*manufacturer specific*												
210	*manufacturer specific*												
211	*manufacturer specific*												
212	*manufacturer specific*												
213	*manufacturer specific*												

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
214	*manufacturer specific*												
215	*manufacturer specific*												
216	*manufacturer specific*												
217	*manufacturer specific*												
218	*manufacturer specific*												
219	*manufacturer specific*												
220	*manufacturer specific*												
221	*manufacturer specific*												
222	*manufacturer specific*												
223	*manufacturer specific*												
224	*manufacturer specific*												
225	*manufacturer specific*												
226	*manufacturer specific*												
227	*manufacturer specific*												
228	*manufacturer specific*												
229	*manufacturer specific*												
230	*manufacturer specific*												
231	*manufacturer specific*												
232	*manufacturer specific*												
233	*manufacturer specific*												
234	*manufacturer specific*												
235	*manufacturer specific*												
236	*manufacturer specific*												
237	*manufacturer specific*												
238	*manufacturer specific*												
239	*manufacturer specific*												
240	*manufacturer specific*												
241	*manufacturer specific*												
242	*manufacturer specific*												
243	*manufacturer specific*												
244	*manufacturer specific*												
245	*manufacturer specific*												
246	*manufacturer specific*												
247	*manufacturer specific*												
248	*manufacturer specific*												
249	*manufacturer specific*												
250	*manufacturer specific*												
251	*manufacturer specific*												
252	*manufacturer specific*												

Event Code	Name	Description	Standard Event Log	Fraud Detection Log	Disconnector Control Log	M-Bus Event Log	M-Bus Control Log 1	M-Bus Control Log 2	M-Bus Control Log 3	M-Bus Control Log 4	Power Quality Event Log	Communication Log	Mandatory/optionl
253	*manufacturer specific*												
254	Load profile cleared	Any of the profiles cleared. NOTE: If it appears in Standard Event Log then any of the E-load profiles was cleared. If the event appears in the M-Bus Event log then one of the M-Bus load profiles was cleared	x			x							M
255	Event log cleared	Indicates that the event log was cleared. This is always the first entry in an event log. It is only stored in the affected event log.	x	x	x	x	x	x	x	x	x		M

Table 47: Event Codes

11. Appendix: Attribute restrictions used in IDIS package 2

The following specifications are necessary to achieve semantic interoperability in IDIS package 2. The additional specifications do not create any conflict with the specifications of the Interface Classes.

11.1 Send_destination_and_method (Push Setup Class, IC 40)

destination (octet-string) element containing the target address where the data has to be sent

IPv6 address and port number:

for the IP address the canonical form of RFC 5952, sect. 4 is used. Further, the IP address is delimited by brackets and the port number separated by a colon (comp. sect. 6 of RFC 5952).

Format: [x:x:x:x:x:x:x:x]:y

The 128 bit IP address is divided into 16-bit pieces (most significant piece left) and each piece is encoded into a decimal number (x). x is represented by up to 5 ASCII digits (leading zeros are omitted). The port number (y) is decimal encoded (0..65535) and represented by up to 5 ASCII digits (leading zeros are omitted). The dots (“.”), the colon (“:”) and the brackets (“[“, “]”) are ASCII encoded. The address always contains all 8 pieces; i.e. pieces which are 0 are not suppressed.

IPv4 address and port number:

the dotted representation is used: x.x.x.x:y

The 32 bit IP address is divided into 4 octets (most significant octet left) and each octet is encoded into a decimal number (x). x is represented by up to 3 ASCII digits (leading zeros are omitted). The port number (y) is decimal encoded (0..65535) and represented by up to 5 ASCII digits (leading zeros are omitted). The dots (“.”) and the colon (“:”) are ASCII encoded.

HDLC:
Contains the logical_name of the HDLC setup object, octetstring(6).

SMS:
The phone number is ASCII encoded, first digit left, only numbers, no blanks.

12. Appendix: New DLMS/COSEM elements

The following section contains new DLMS/COSEM elements which are in the process to be included into Blue Book (BB) of the DLMS-UA and which are used in IDIS package 2.

12.1 New Blue Book Elements

12.1.1 4.8.7 NTP setup (class_id: 100, version: 0)

This IC allows setting up time synchronization using the NTP protocol as defined in RFC1305 and RFC 2030.

NTP Setup		**0...n**	**class_id = 100, version = 0**			
Attributes		***Data type***	***Min.***	***Max.***	***Def.***	**Short name**
1. logical_name	(static)	octet-string				x
2. activated	(static)	boolean				x + 0x08
3. server_address	(static)	octet-string				x + 0x10
4. server_port	(static)	long-unsigned			123	x + 0x18
5. authentication_method	(static)	enum				x + 0x20
6. authentication_keys	(static)	array				x + 0x28
7. client_key	(static)	octet-string				x + 0x30
Specific methods		***m/o***				
1. synchronize_time (data)		m				x + 0x38
2. add_authentication_key (data)		o				x + 0x40
3. delete_authentication_key (data)		o				x + 0x48

Attribute description

logical_name	Identifies the “NTP setup” object instance. See section 12.1.2.1.
activated	Defines if the NTP time synchronization is active or not. Synchronization active = TRUE
server_address	Defines the NTP server address as an octet string. This server address can be a name, which must be resolvable by the primary DNS or the secondary DNS. In the case when it is directly the IP address of the server, which is specified here, it shall be a string in dotted format. Example: 163.187.45.87.
server_port	Defines the value of the UDP port related to this protocol. By default, this value is the NTP port number ID assigned by IANA: ntp 123/udp Network Time Protocol

authentication_ method	Defines the authentication mode used for NTP protocol enum: (0) no_security (not recommended) (1) shared_secrets *(2) auto_key_IFF (not supported by IDIS pack2)* *(3) Private Certificate Identity Scheme ? (not supported by IDIS pack2)* *(4) Trusted Certificate Identity Scheme ? (not supported by IDIS pack2)* *(5) Guillou-Quisquater Identity Scheme ? (not supported by IDIS pack2)* *(6) Mu–Varadharajan Identity Scheme ? (not supported by IDIS pack2)*

authentication_keys	Contains the necessary symmetric keys if shared secrets mode of authentication is used.
	authentication_keys ::= array authentication_key
	authentication_key ::= structure
	{
	key_id double-long
	key octet-string
	}

client_key	Specifies the client key (NTP server public key) for NTP auto key authentication mechanism using IFF authentication scheme (auto_key_IFF).

Method description

synchronize (data)	Synchronizes the time with the NTP server. data ::= integer(0)

add_authentication_key (data)	Adds a new symmetric authentication key to authentication key array.
	data ::= structure
	{
	key_id double-long
	key octet-string
	}

delete_authentication_key (data)	Deletes a symmetric authentication key from the key array. The key to be deleted is identified by its key_id. data ::= double-long

12.1.2 Relation to OBIS

12.1.2.1 NTP setup objects

Instances of the IC "NTP setup" handle all information related to the setup of the NTP time synchronization service.

Add the following line to the table

NTP setup	100, NTP setup	0	*b*	25	10	0	255

Index