IDIS
INTEROPERABILITY SPECIFICATION
RELEASE 1

# Package 1
# PLC Profile

**Edition 1.0, 2010**

Excerpt w3.5

# 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)

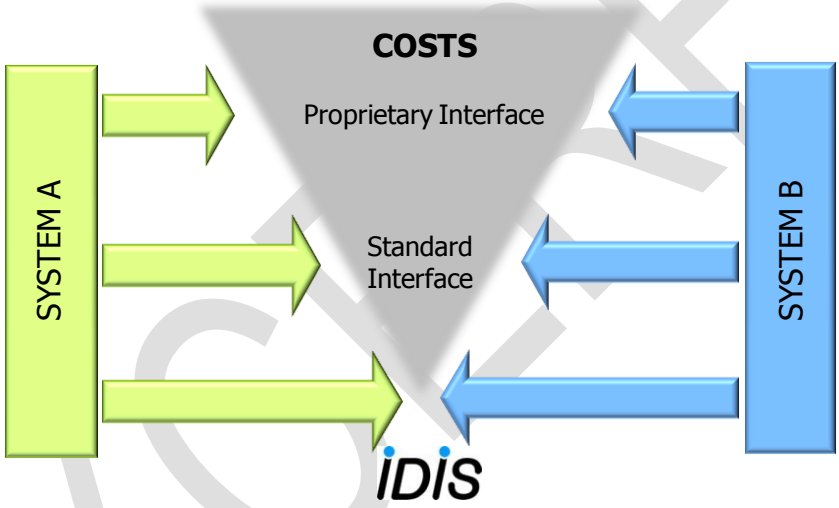



*Figure 1: Costs to integrate and operate different types of interfaces*

## 2.2 Scope of this document

This document is part of the IDIS Interoperability Package 1. It specifies the functionality of an IDIS device integrated into a PLC (powerline carrier) communication network.

The functionality of the IDIS device is based on the DLMS/COSEM standards. PLC communication is based on Spread-frequency Shift Keying as described in the IEC 61334-5-1 standard.

# 3. Introduction

## 3.1 Referenced Documents

| Ref. | Title |
|---|---|
| DLMS UA 1000-2 Ed. 7.0:2010 | *DLMS/COSEM Architecture and Protocols, the "Green Book"* |
| DLMS UA 1000-1 Ed. 10.0:2010 | *COSEM Identification System and Interface Classes, the "Blue Book" Ed. 10 is in pre-release state.* |
| IDIS P1-OBJ ed1.0 | *IDIS Package 1, Smart metering Objects* |
| 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* |
| EN 13757-5:2008 | *Wireless meter readout — Communication systems for meters and remote reading of meters — Part 5: Relaying* |
| IEC 61334-4-32 Ed. 1.0:1996 | *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 32: Data link layer – Logical link control (LLC)* |
| IEC 61334-4-511 Ed. 1.0:2000 | *Distribution automation using distribution line carrier systems – Part 4-511: Data communication protocols – Systems management – CIASE protocol* |
| IEC 61334-4-512 Ed. 1.0:2001 | *Distribution automation using distribution line carrier systems – Part 4-512: Data communication protocols – System management using profile 61334-5-1 – Management Information Base (MIB)* |
| IEC 61334-5-1 Ed. 2.0:2001 | *Distribution automation using distribution line carrier systems – Part 5-1: Lower layer profiles – The spread frequency shift keying (S-FSK) profile* |
| 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 62056-53 Ed. 2.0:2006 | *Electricity metering – Data exchange for meter reading, tariff and load control – Part 53: COSEM Application layer* |
| IEC 62056-61 Ed. 2.0:2006 | *Electricity metering – Data exchange for meter reading, tariff and load control – Part 61: Object identification system (OBIS)* |
| IEC 62056-62 Ed. 2.0:2006 | *Electricity metering – Data exchange for meter reading, tariff and load control – Part 62: Interface classes* |

## 3.2 Terms, Definitions and Abbreviations

| Abbreviation | Explanation |
|---|---|
| AA | Application Association |
| AARE | Application Association Response |
| AARQ | Application Association ReQuest |
| ACSE | Association Control Service Element |
| APDU | Application Protocol Data Unit |
| ASE | Application Service Element |
| A-XDR | Adapted Extended Data Representation |
| class_id | Interface class identification code |

| Abbreviation | Explanation |
|---|---|
| COSEM | Companion Specification for Energy Metering |
| COSEM object | An instance of a COSEM interface class |
| DC | Data Concentrator |
| DLMS | Device Language Message Specification |
| ERP | Enterprise Resource Planning |
| FC | Frame Counter |
| GCM | Galois/Counter Mode, an algorithm for authenticated encryption with associated data |
| GMT | Greenwich Mean Time |
| 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 |
| OBIS | OBject Identification System |
| PDU | Protocol Data Unit |
| SAP | Service Access Point |
| L_SAP | Link layer Service Access Point |

## 3.3 Revision History

| Version | Date | Author | Comment |
|---|---|---|---|
| Edition 1 | 01.09.2010 | IDIS Specs Team | Initial version |

# 4. IDIS Conformance Testing

IDIS components are tested for conformity according to the rules set be the IDIS Industry Association.

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

- the *Extensions* 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 1

IDIS 1
No 100820

Device supporting Basic, Disconnector and Multi-Utility functionality of IDIS package 1

IDIS 1DM
No 100840

Device supporting Basic, Disconnector. Load Management and Multi-utility functionality of IDIS package 1

IDIS 1DLM
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.

# 5. IDIS System Architecture

## 5.1 Basic principles

IDIS primeraly supports PLC communication between the electricity meter and the Data Concentrator. The green parts shownn in Figure 2 are supported by IDIS.

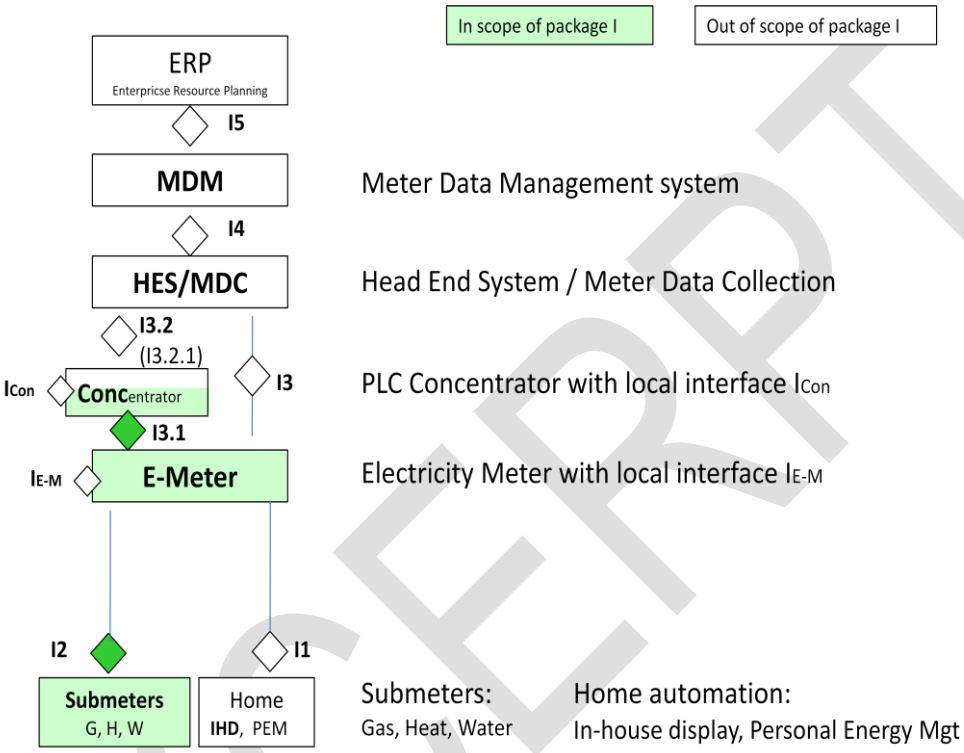



*Figure 2: System architecture supported by IDIS package 1*

NB: The following interfaces are *NOT* in scope of IDIS package1: I5, I4, I3.2, I3, I1, and the local interfaces: Icon, IE-M

## 5.2 Interface I3.1 (PLC)

IDIS package 1 supports PLC communication as specified in the following documents:

- IEC 61334-5-1
- IEC 61334-4-511
- DLMS UA 1000-2 Ed. 7.0

Figure 3 gives an overview on the communication architecture used in IDIS (see also DLMS UA 1000-1 Ed. 10.0:2010)

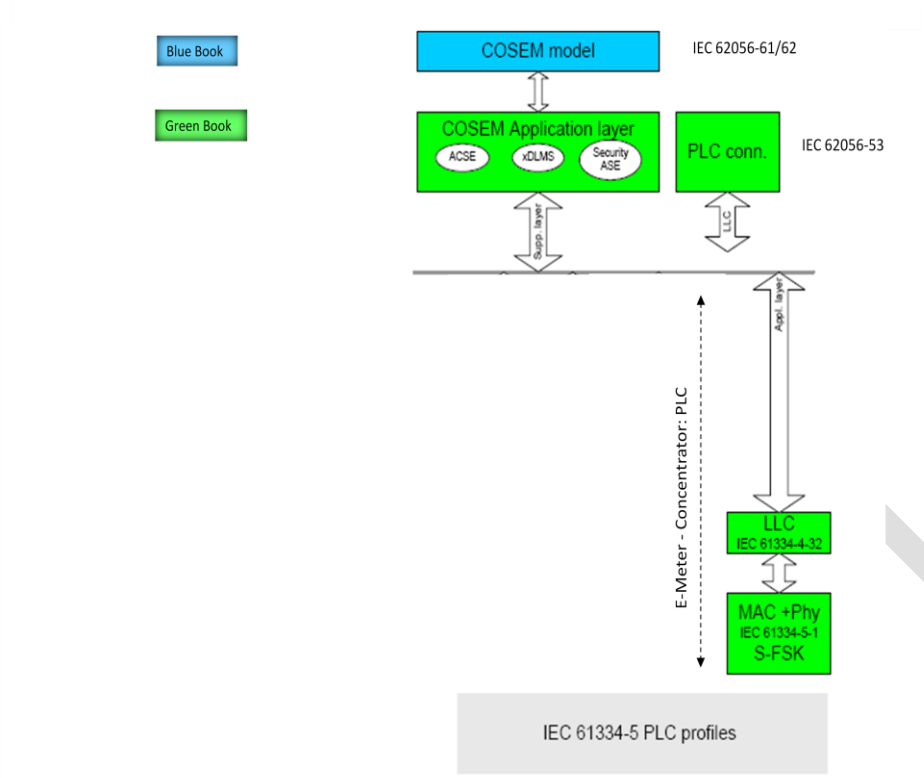



*Figure 3: PLC communication supported by IDIS package 1*

## 5.3 Interface I3.2.1 (DC internal, optional)

IDIS package 1 offers an *optional* application interface to the Java runtime environment on the Data Concentrator. The runtime environment provides COSEM services GET, SET, and ACTION to access the devices in the PLC network.

NB: The specification of the Java applications that use the Java API is not part of IDIS package 1. These Java applications and the interface between the DC and the HES is in the responsibility of the HES/MDM system provider.

## 5.4 Interface I2 (submeters)

*Section deleted in excerpt*

### 5.4.1 Wired M-Bus

*Section deleted in excerpt*

### 5.4.2 Wireless M-Bus

*Section deleted in excerpt*

# 6. Use Cases supported by IDIS package 1

The following Use Cases are supported by IDIS Package 1.

| | "Open Meter" Use Case | Description | IDIS Package 1 specific remarks |
|---|---|---|---|
| UC1 | Meter Registration | Process of incorporating devices (E-meters, submeters, ...) into the system. | • Automatic registration of the E-meter within the PLC network. Submeters must be configured and registered manually.<br>• Registration at the HES or MDM level is not part of package 1. |
| 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)<br>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)<br>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 customer. | • Remote controlled (E,G)<br>• Time (local) controlled (E,G)<br>• Load (local) controlled (E) |
| UC6 | Clock Synchronization | Process of adjusting the internal clock of the metering equipment | • For E-meters only<br>• Source of sync<br>PLC: HES via DC |
| UC7 | Quality of Supply | Process of supervising Power Outages, Sags and Swells, | • Event-Logs and counters<br>• 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<br>• Time (local) controlled<br>• Load (local) controlled |
| UC9 | Firmware update | Process of downloading new firmware to a device | • For E-meters only<br>• Only remote upgrade, interoperability restricted to the downloading process |
| UC10 | Meter supervision | Process of supervising any events which could comprise the meter and the system. | • For E-meters only<br>• Security event logs |

*Table 1 Use Cases supported by IDIS package 1*



## 6.1 Meter Registration

Automatic Registration of the E-meter at the DC is supported by the Discover and registration service as described in DLMS UA 1000-2 Ed. 7.0 sect. 10.4.5.2./3.

A crucial parameter echanged between the meter and the DC is the “System Title” . IDIS encodes the COSEM Logical Device name into the System Title.

### 6.1.1 System Title

*Section deleted in excerpt*

Example System Title:

*Section deleted in excerpt*

### 6.1.2 COSEM Logical Device Name

*Section deleted in excerpt*

## 6.2 Remote Tariff Programming

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.

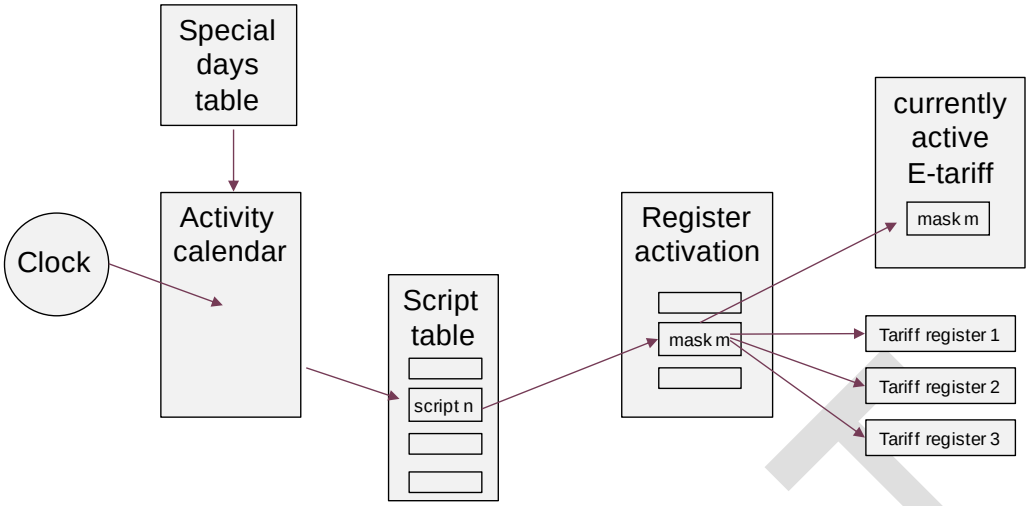



*Figure 4: COSEM objects managing tariffication*

In addition to the specifications provided in DLMS UA 1000-1 Ed. 10.0:2010 the follwing 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:

*Section deleted in excerpt*

## 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 follows:

| 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 2: Assignment of tariffs to scripts*

#### *6.2.2.1.1 Default tariff*

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

### 6.2.3 Register activation

*Section deleted in excerpt*

### 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”:

*Section deleted in excerpt*

## 6.3 Meter Reading on Demand

### 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 specificed Total Registers defined in IDIS P1-OBJ ed1.0.
- 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 P1-OBJ ed1.0.

#### 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.

**Load Profile 1 (1-0:99.1.0.255)**

*Section deleted in excerpt*

**Load Profile 2 (1-0:99.2.0.255)**

*Section deleted in excerpt*

## 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)**

*Section deleted in excerpt*

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

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

*Section deleted in excerpt*

## 6.3.3 Load Profile for general metering

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

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

| | |
|---|---|
| min capacity: | 13 months, 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[1]: 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. 7.0, p210) is used.<br>for values: the same as the previous<br>for clock: previous + capture period[2] |

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

[2] 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.

### 6.3.4 Profile_status

The status of a buffer entry consists of a one byte (type *Unsigned*) where the bits have the following meaning:

Bit 7 **Power down**: This bit is set to indicate that an all-phase power failure occurred.

Bit 6 Reserved.

Bit 5 **Clock adjusted**: The bit is set when clock has been adjusted more than the synchronization limit. At the same time the “Data not valid” flag is set because the capture period deviates from its nominal lengths and may not be used for billing.

Bit 4 Reserved.

Bit 3 **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 in winter.

*Section deleted in excerpt*

## 6.4 Meter Reading for Billing

The meter provides the metering objects as described in 6.3 also for billing purposes. Scheduled meter reading for billing must be supported by the DC applications. The DC applications are out of the scope of IDIS package 1 (comp. 5.3)

## 6.5 Meter Disconnection and Reconnection

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)<br>Allows to supervise the instantaneous current or the sliding demand and the execute 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)<br>Allows to supervise the instantaneous or the average value of the current per phase. | L1: logical_name: 1-0:31.4.0.255<br>L2: logical_name: 1-0:51.4.0.255<br>L3: logical_name: 1-0:71.4.0.255 |

*Section deleted in excerpt*

## 6.6 Meter Clock Synchronisation

The time in the electricity meters is set/synchronised by applying the SET service to the attribute "time" of the "clock" object (logical_name: 0-0:1.0.0.255). In IDIS package 1 the time is regularely set by the DC.

The time attribute (*date_time* format; octet-string(12) ) can be written in two ways:

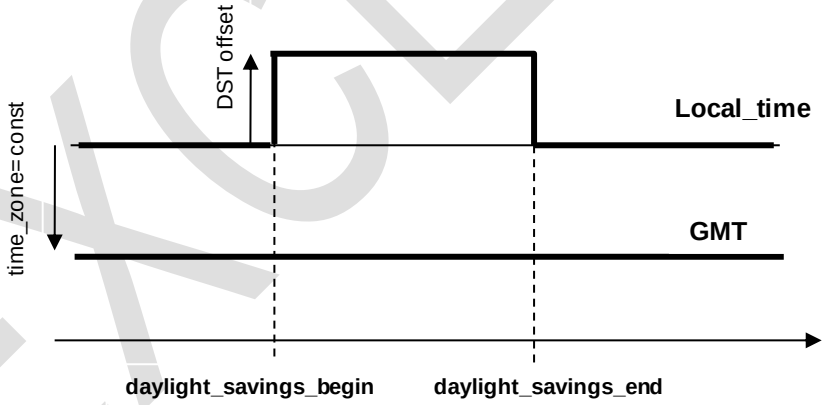
| Year, month, day of month, day of week, hour, minute, second, hundredths of seconds | deviation | Clock status | Supported by the meter |
|---|---|---|---|
| the meter's local time | 0x8000 (not specified) | 0xFF | mandatory |
| the system's local time | Deviation of the system's local time to GMT | 0x00 | optional |

*Table 3: 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 must write these attributes explicitely or set them to "not specified" (0xFF) when writing the time.

### 6.6.1 Relation between the different time parameters

The following clarifications concern the time parameters as used in DLMS UA 1000-1 Ed. 10.0:2010.




*Section deleted in excerpt*

## 6.7 Quality of Supply

The quality of supply is supervised by means of the following event logs:

| | |
|---|---|
| Power Failure Event Log (class_id 7)<br>registrating the durations of power failures in any phase | logical_name: 1-0:99.97.0.255 |

| | |
|---|---|
| Power Quality Log (class_id 7)<br>registrating the power quality relevant events | logical_name: 0-0:99.98.4.255 |

The event identifiers are defined in IDIS P1-OBJ ed1.0.

## 6.8 Load Management by Relay

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

*Section deleted in excerpt*

## 6.9 Firmware Update

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 version (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.

*Section deleted in excerpt*

### 6.9.1 Changing the system title

If – as part of the firmware update – the system title (comp. 6.1.1) is changed, then the IDIS server will pass to status NEW and issue an alarm with Alarm Descriptor Bit 0 set (comp. 7.3.2.4). The DC will register the meter with the new firmware as an new device (comp. 8.4.1).

## 6.10 Meter supervision

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

| | |
|---|---|
| Standard Event log (class_id 7)<br>Containing event codes. At least 100 entries are supported. | logical_name: 0-0:99.98.0.255 |
| Fraud Detection log (class_id 7)<br>Containing fraud event codes. At least 30 entries are supported. | logical_name: 0-0:99.98.1.255 |

The event identifiers are defined in IDIS P1-OBJ ed1.0.

# 7. E-Meter Functionality

## 7.1 Data Model

The entire functionality of the IDIS meter is modelled by means of COSEM objects as described in DLMS UA 1000-1 Ed. 10.0:2010.

IDIS P1-OBJ ed1.0 (excerpt in Figure 5) provides a complete list of the mandatory and optional objects used in IDIS package 1. The objects are described in all details, in particular:

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

are given. For an extract of IDIS P1-OBJ ed1.0, see Figure 5.

*An IDIS server and system must support ALL IDIS objects (mandatory and optional) as defined in* IDIS P1-OBJ ed1.0.

## 7.2 IDIS Meter customisation

Every IDIS meter must support the complete set of BASIC objects. Further, the minimal functionality may be extended with any combination of Disconnector, Load Management and/or 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 P1-OBJ ed1.0). 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 COSEM objects are mandatory for every IDIS package 1 device. Not all rated registers are mandatory. For details on the mandatory rated registers comp. 6.3.1.

*Section deleted in excerpt*

*Table 4 BASIC(mandatory) IDIS objects*

### 7.2.2 Extension D objects

The follwing objects are foreseen for all IDIS devices supporting the Disconnector functionality. Detailed information on mandatory/optional objects and attributes can be found in IDIS P1-OBJ ed1.0.

*Section deleted in excerpt*

*Table 5 Extension D IDIS objects*

### 7.2.3 Extension L objects

The follwing objects are foreseen for all IDIS devices supporting the Load Management functionality. Detailed information on mandatory/optional objects and attributes can be found in IDIS P1-OBJ ed1.0.

*Section deleted in excerpt*

*Table 6 Extension L IDIS objects*

### 7.2.4 Extension M objects

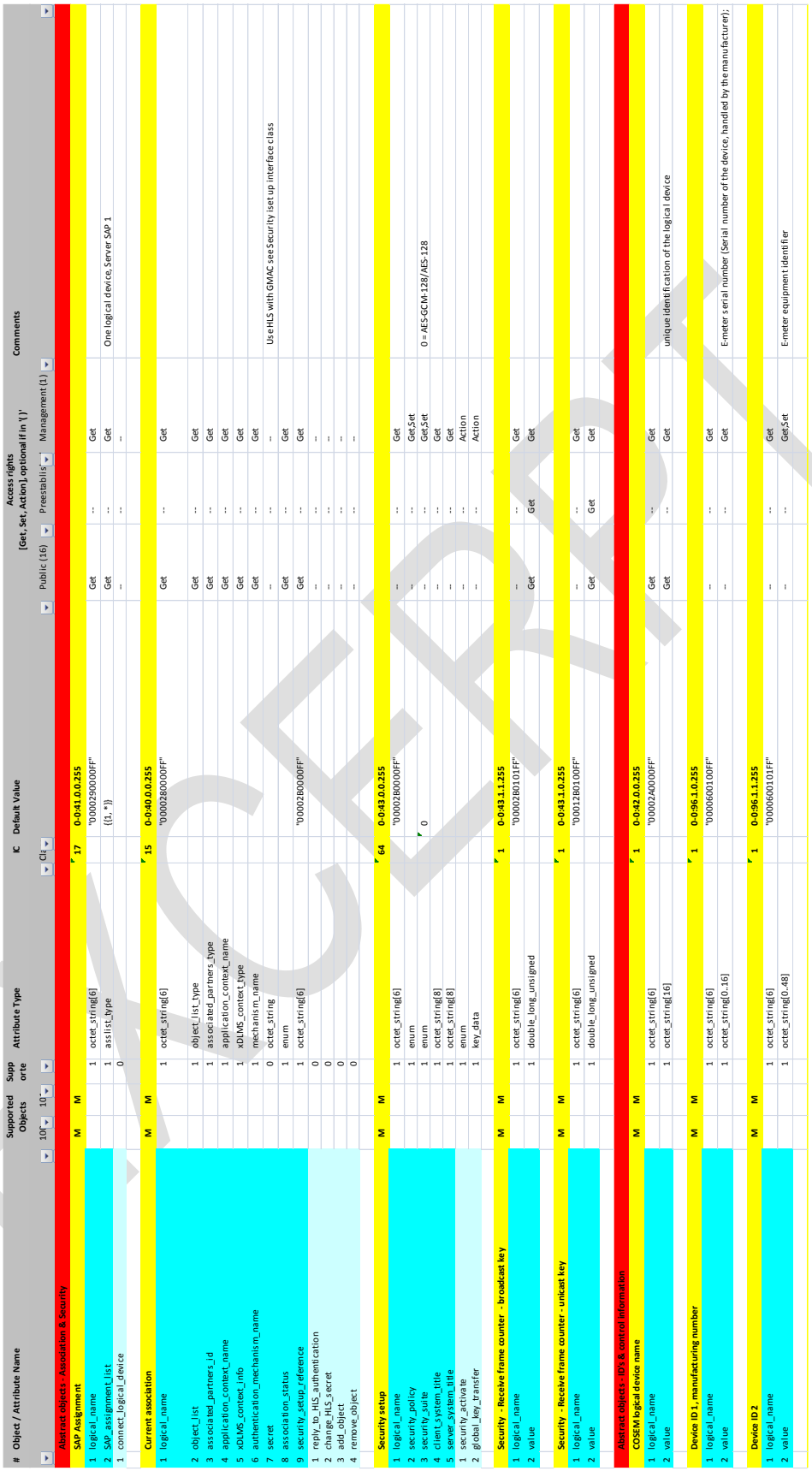
The follwing objects are foreseen for all IDIS devices supporting the Multi-Utility (restricted to M-bus for IDIS package 1) functionality. Detailed information on mandatory/optional objects and attributes can be found in IDIS P1-OBJ ed1.0.

*Section deleted in excerpt*

*Table 7 Extension M IDIS objects*

### 7.2.5 Optional objects

Optional objects according to IDIS P1-OBJ ed1.0. may be added by the IDIS device manufacturer. They must be tested as described in sect. 4.



| # | Object / Attribute Name | Supported Objects | Supported | Attribute Type | IC | Default Value | Access rights [Get, Set, Action] optional if in '()' | | | Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Public (16) | Preestablis | Management (1) | |
| | **Abstract objects - Assodation & Security** | | | | | | | | | |
| | **SAP Assignment** | M | M | | 17 | 0-0:41.0.0.255 | | | | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000290000FF" | Get | -- | Get | |
| 2 | SAP_assignment_list | | | 1 assist_type | | {(1, *)} | Get | -- | Get | One logical device, Server SAP 1 |
| 1 | connect_logical_device | | | 0 | | | -- | -- | -- | |
| | **Current association** | M | M | | 15 | 0-0:40.0.0.255 | | | | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000280000FF" | Get | -- | Get | |
| 2 | object_list | | | 1 object_list_type | | | Get | -- | Get | |
| 3 | associated_partners_id | | | 1 associated_partners_type | | | Get | -- | Get | |
| 4 | application_context_name | | | 1 application_context_name | | | Get | -- | Get | |
| 5 | xDLMS_context_info | | | 1 xDLMS_context_type | | | Get | -- | Get | |
| 6 | authentication_mechanism_name | | | 1 mechanism_name | | | Get | -- | Get | |
| 7 | secret | | | 0 octet_string | | | -- | -- | -- | Use HLS with GMAC, see Security iset up interface class |
| 8 | association_status | | | 1 enum | | | Get | -- | Get | |
| 9 | security_setup_reference | | | 1 octet_string[6] | | "0000280000FF" | Get | -- | Get | |
| 1 | reply_to_HLS_authentication | | 0 | | | | -- | -- | -- | |
| 2 | change_HLS_secret | | 0 | | | | -- | -- | -- | |
| 3 | add_object | | 0 | | | | -- | -- | -- | |
| 4 | remove_object | | 0 | | | | -- | -- | -- | |
| | **Security setup** | M | M | | 64 | 0-0:43.0.0.255 | -- | -- | Get | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000280000FF" | -- | -- | Get | |
| 2 | security_policy | | | 1 enum | | 0 | -- | -- | Get,Set | |
| 3 | security_suite | | | 1 enum | | | -- | -- | Get,Set | 0 = AES-GCM-128/AES-128 |
| 4 | client_system_title | | | 1 octet_string[8] | | | -- | -- | Get | |
| 5 | server_system_title | | | 1 octet_string[8] | | | -- | -- | Get | |
| 1 | security_activate | | | 1 enum | | | -- | -- | Action | |
| 2 | global_key_transfer | | | 1 key_data | | | -- | -- | Action | |
| | **Security - Receive frame counter - broadcast key** | M | M | | 1 | 0-0:43.1.1.255 | | | | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000280101FF" | -- | -- | Get | |
| 2 | value | | | 1 double_long_unsigned | | | Get | Get | Get | |
| | **Security - Receive frame counter - unicast key** | M | M | | 1 | 0-0:43.1.0.255 | | | | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000280100FF" | -- | -- | Get | |
| 2 | value | | | 1 double_long_unsigned | | | Get | Get | Get | |
| | **Abstract objects - IDIS & control information** | | | | 1 | 0-0:42.0.0.255 | | | | |
| | **COSEM logical device name** | M | M | | 1 | "0000240000FF" | Get | -- | Get | |
| 1 | logical_name | | | 1 octet_string[6] | | | Get | -- | Get | |
| 2 | value | | | 1 octet_string[16] | | | Get | -- | Get | unique identification of the logical device |
| | **Device ID 1, manufacturing number** | M | M | | 1 | 0-0:96.1.0.255 | | | | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000600100FF" | -- | -- | Get | |
| 2 | value | | | 1 octet_string[0..16] | | | -- | -- | Get | E-meter serial number (Serial number of the device, handled by the manufacturer); |
| | **Device ID 2** | M | M | | 1 | 0-0:96.1.1.255 | | | | |
| 1 | logical_name | | | 1 octet_string[6] | | "0000600101FF" | -- | -- | Get | |
| 2 | value | | | 1 octet_string[0..48] | | | -- | -- | Get,Set | E-meter equipment identifier |

*Figure 5 Extract of IDIS P1-OBJ ed1.0*

## 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, these events may also be used to set and clear errors as well as to trigger alarms.

### 7.3.1 Events

The event identifiers are defined in IDIS P1-OBJ ed1.0.

### 7.3.2 Alarms

See also 8.4.1.

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

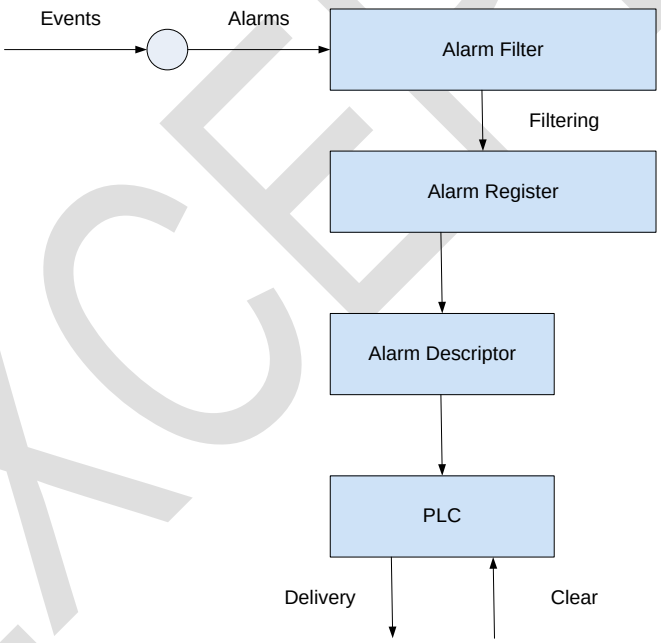



*Figure 6: Alarm Reporting procedure*



*Section deleted in excerpt*

#### 7.3.2.1 COSEM Objects supporting Alarms

| | |
|---|---|
| Alarm Register (class_id 1) | Logical_name: 0-0:97.98.0.255 |
| Alarm Filter (class_id 1) | Logical_name: 0-0:97.98.10.255 |

#### 7.3.2.2 Assignment of Alarm Register bits

*Section deleted in excerpt*

*Table 8 Assignment of Alarm register bits*

#### 7.3.2.3 Assignment of Alarm Filter bits

Alarm Filter (double_long_unsigned) has the same structure as the Alarm Register. A set bit (logical 1) in the Alarm Filter means that the corresponding alarm is activated.

#### 7.3.2.4 Assignment of Alarm Descriptor bits

The S-FSK profile provides the transport of an alarm from the meter to the DC by means of the Discovery Service. The Alarm Descriptor is a parameter of the Discover service (comp. DLMS UA 1000-2 Ed. 7.0, sect 10.4.5.2) carrying the alarming information.

*Section deleted in excerpt*

*Table 9 Assignment of Alarm Descriptor bits*

Bit 0 indicates that the PLC module is in status “new”. Bit 1 to 6 are the same as in the Alarm Register bits 0 to 5. Bit 7 indicates that an Extended Alarm was encountered where the details can be found in the bit positions 6 to bit 31 of the COSEM object Alarm Register.

# 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 Pre-estblished Clients (SAP: 102), Public Clients (SAP: 016), and Management Clients (SAP001) as illustrated in Figure 7. Details on the use of the different clients can be found in section 8.2.2.

Network Management is supported by the client and server CIASE connected to SAP 000.

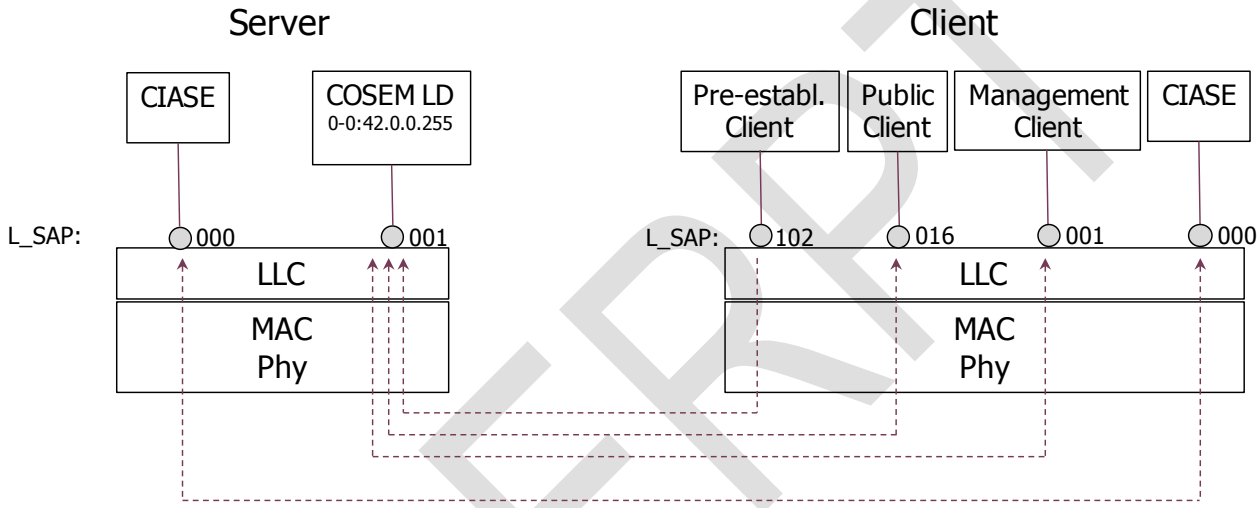



*Figure 7 IDIS Client and Server model*

## 8.2 Application Layer

The E-Meter communicates with the upper system (via I3.1, I3) using the IEC 62056-53 COSEM Application Layer with extension documented in DLMS UA 1000-2 Ed. 7.0.

### 8.2.1 Minimal set of services

*Logical name* services are supported. The Conformance Block (IEC 62056-53) defines the minimal set of supported application layer services:

*Section deleted in excerpt*

#### 8.2.1.1 The Invoke-Id-And-Priority byte

Is handled according to DLMS UA 1000-2 Ed. 7.0. In particular, Bit 6 (service_class) must be set

*Section deleted in excerpt*

## 8.2.2 Minimal set of Associations

At least the following 3 Associations must be supported:

*Section deleted in excerpt*

*Table 10 Minimal set of supported associations*

The list of COSEM objects in IDIS P1-OBJ ed1.0 explicitly assigns clients and access rights to all attributes used in IDIS package 1.

*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 Power-down

For the PLC comm. port:
the entire context of the public client , the pre-established client and the management-client are saved in non-volatile memory. The contexts are automatically re-established upon power up.

For the local (optical) port:
A power-down will close automatically any association on the local port.

### 8.2.2.2 Pre-established Association

Used by the pre-established client.

The application context is the same as for the management client (except for the parameters which are negotiable between the client and server). In particular:

- max receive pdu_size= 239
- max send pdu size= 239
- DLMS version nr= 6
- Quality of service= not used
- Cyphering info= not used
- Conformance= SET, ACTION (invoke id: bit6 =0, no confirmation)
- Application context name= 3 (logical name + 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 P1-OBJ ed1.0.

#### 8.2.2.3 Association Release Request RLRQ

*Section deleted in excerpt*

#### 8.2.2.4 Application association object

*Section deleted in excerpt*

#### 8.2.2.5 Handling lost Associations

*Section deleted in excerpt*

#### 8.2.2.6 Associations on different communication ports

*Section deleted in excerpt*

### 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 are specified in case of an erroneous condition (condition NOT fulfilled)

*Section deleted in excerpt*

*Table 11 Error events associated to the AARQ service*

#### 8.2.3.3 Errors related to the Get/Set/Action services

*Section deleted in excerpt*

*Table 12 Error events associated to GET, SET and ACTION*

#### 8.2.3.4 Errors related to the RLRQ service

| Condition NOT fulfilled in the service | Action performed by the server |
|---|---|
| Association OPEN | RLRE.reason = normal<br>Altenatively,<br>Exception response(state-error=service-not-allowed, service- |

| | |
|---|---|
| | error=operation-not-possible) |
| User Information = RECEIVED | RLRE.reason = not_finished |

*Table 13 Error events associated to the RLRQ service*

#### 8.2.3.5 Errors in secured services

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

##### *8.2.3.5.1 Errors in the secured AARQ service*

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

*Table 14 Error events associated to the secured AARQ service*

##### *8.2.3.5.2 Errors in the secured RLRQ service*

| 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 15 Error events associated to the secured RLRQ service*

## 8.3 Lower layers and CIASE for PLC communication

The following sections contain clarifications to the existing standards necessary to achieve interoperability on the PLC network.

The following conventions apply:

M mandatory

O optional

U usage dependent (the presence of the corresponding parameter depends on the application)

- parameter is not used

### 8.3.1 IEC 61334-5-1 Physical layer options

The options used in IDIS package 1 are specified with reference to the sections in IEC 61334-5-1.

The following physical layer services are used:

- P_Data
- P_Sync

**Section 2.3 Frequency spread**

- $f_M$ = 63.3 kHz
- $f_S$ = 74 kHz
- $f_M$, $f_S$ transmission frequency tolerance = +/- 0.5%

**Section 2.4.1 Performance test:**
*Section deleted in excerpt*

**Section 3.2.2 Bit repetition frequency:**
*Section deleted in excerpt*

**Section 3.4.1.1 P_Data services**

| ServicePrimitives | .request | .confirm | .indication |
|---|---|---|---|
| P_Data | M | M | M |
| All the parameters | M | M | M |

**Section 3.4.1.2 P_Sync services**

| ServicePrimitives | .request | .confirm | .indication |
|---|---|---|---|
| P_Sync | M | M | M |
| All the parameters | M | M | M |

**Section 7.5.4 Table 3.5.4**

The following amendments are used:

- The 6th transition includes (LFS or S_IDL to LFS); it only includes LFS in the initial state.
- The 15th transition (S_RPF_R) presents a Sync_conf variable. This should be disregarded.

## 8.3.2 IEC 61334-5-1 MAC layer options

The options used in IDIS package 1 are specified with reference to the sections in IEC 61334-5-1.

The following MACl layer services are used:

- MA_Data
- MA_Sync

**Section 4.1.3.1 and Sections 4.1.4 to 4.1.6 MA_Data services**

*Section deleted in excerpt*

The following parameters can be selected:

*Section deleted in excerpt*

**Sections 4.1.3.2 and 4.1.7.2 MA_Sync services:**

| ServicePrimitives | .request | .confirm | .indication |
|---|---|---|---|
| MA_Sync | - | - | M |
| Synchro State | - | - | M |
| Synchro Loss Cause | - | - | C |
| Source Address | - | - | C |
| Destination Address | - | - | C |

O (optional) in the standard. In this case, C (conditional), as the values are only valid if the Synchro State value is Synchro Lost. As the service is local, it has no impact on the network.

The following parameters can be selected:

*Section deleted in excerpt*

**Section 4.2.3.5.1FCS calculation method**

A cyclic redundancy code (CRC) is used to generate the frame control sequence, known as FCS.

The CRC is calculated from the MA_PDU, from which the two NS bytes are removed. For the precise composition of the MA_PDU, see the diagram below.

Example of a frame consisting of a single subframe (synchronisation frame):

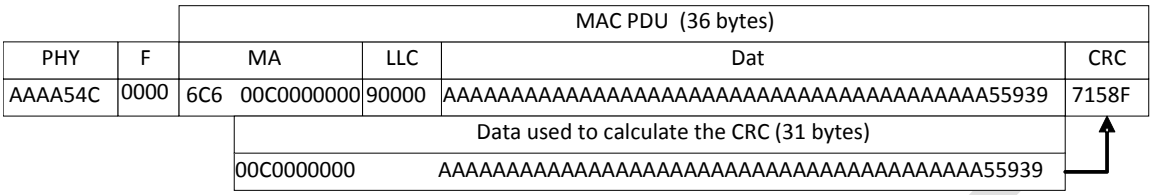



*Figure 8 Example of the CRC of a MAC frame*

The result of the CRC calculation for the above example is 0x7158F9.
The reverse polynomial (0xD3B6BA) is used to calculate the CRC.

The algorithm used is as follows:

*Section deleted in excerpt*

### 8.3.2.1 Address values

#### *8.3.2.1.1 Individual addresses*

The PLC meters have a MAC address between 001h and BFFh (i.e. a maximum of 3071 addresses). The addresses are distributed by the concentrator (known as the Initiator) in time order (the address of the first meter registered will be address 1, etc.).

The MAC addresses of the concentrators are between C00h and DFFh, i.e. a maximum of 511 concentrator addresses.

The way in which the MAC addresses of the concentrators are assigned depends on the concentrator application and not on the PLC profile; for example, the addresses can be assigned by the information system.

#### *8.3.2.1.2 Group addresses*

The NO-BODY address is the address of group 000.

*Section deleted in excerpt*

## 8.3.3 IEC 61334-4-32 LLC layer Options

The options used in IDIS package 1 are specified with reference to the sections in IEC 61334-4-32

Only one LLC layer service **is used** to transport the apdus generated by the application layer.

- DL_Data: Main primitive used to send data from a Client to a Server.

The following services are **not used** in IDIS package 1:

- DL_Reply:
- DL_Update Reply:
- DL_Broadcast

**Section 2.2 and following sections: DL_Data services:**

*Section deleted in excerpt*

#### 8.3.3.1 LSAP assignment

The L_SAPs are assigned as described in 8.1.

## 8.3.4 IEC 61334-4-511 CIASE Options

The options used in IDIS package 1 are specified with reference to the sections in IEC 61334-5-1IEC 61334-4-511.

IDIS package 1 uses the two CIASE services:

- Discover
- Register

**Section 7.1**

| ServicePrimitive | .request | .confirm |
|---|---|---|
| Discover | M | M |
| Response Probability | M | - |
| Allowed Time Slots | M | - |
| DiscoverReport Credit | M | |
| ICEqualCredit | M | - |
| Result(+) | | S |
| Number of received invalid frames | | M |
| List of System Titles | | M |
| List of States | | M |
| Result(-)<br>Error | | S<br>M |

List of System Titles (System-Title-List)

*Section deleted in excerpt*

**Section 7.2**

| ServicePrimitive | .request | .confirm |
|---|---|---|
| Register | M | M |
| New System Title(s) | M | - |
| MAC Adress(es) | M | |
| Result(+) | | S |
| Result(-)<br>Error | | S<br>M |

It is important to note that the MAC addresses must be assigned by the concentrator in ascending order starting with 1. This is required by the RepeaterCall mechanism calculation algorithm.

Possible *Error* values (Section 7.3.3)

- other (0),
- Register-mac-address-invalid (1),
- Register-system-title-invalid (2).

**Section 7.3**

```
DiscoverReportPDU::= SEQUENCE {
SEQUENCE OF {System-Title},        -- the first one of this list is the system-title of the reporting system.
alarm-descriptor                   INTEGER(-128..126) OPTIONAL} – alarm-descriptor of the reporting system.
```

## 8.4 PLC Network Management

IDIS supports the following functions for an optimised management of the PLC network:

- Alarming
- Repeater Allocation
- Initiator Allocation
- Ping Service

## 8.4.1 Alarm Management

When alarms (comp. 7.3.2) are generated they are stored in the Alarm Register and are delivered to the Alarm Management System through the appropriate communication channel. Section deleted *in excerpt*

Figure 9 shows the different services of the PLC channel supporting the alarm managment.

Using PLC communication the alarms are raised by S-FSK Alarm delivery. The Alarm Management System - upon receipt of S-FSK Alarm - discovers the devices with Alarm Status using the CIASE Discover service. The Alarm Descriptors are sent to the Alarm Management System as part of the DiscoverReport pdus. If an Extended Alarm Status is indicated the Alarm Management System reads the COSEM object Alarm Register to receive the complete Alarm status. Alarms are cleared with the CIASE ClearAlarm service or with writing to the Alarm Register.

*Section deleted in excerpt*

*Figure 9 The Alarm Management services*

### 8.4.1.1 Physical layer services

The alarm service allows a IDIS server to inform the client that the server is in the alarm state. The client will have to poll the server to find out information or the corresponding alarm state as described in

The service primitives are:

- P_Alarm.request
- P_Alarm.confirm
- P_Alarm.indication

| ServicePrimitives | .request | .confirm | .indication |
|---|---|---|---|
| P_Alarm | M | M | M |
| Result | - | M | - |

Possible Result values:

- OK
- NotOk (not synchronised with the electrical network)

#### *8.4.1.1.1 Server protocol specification*

**Processing the *P_Alarm* request**

When a *P_Alarm* request is received, the physical layer of the server system performs the following operations:

- If the PLC module is not synchronised with the network, the alarm is not sent. The P_Alarm.confirm service primitive is returned with the "NotOk" error.

*Section deleted in excerpt*

**Management of alarms from other servers**

The server module must listen continuously for alarm information.

In receive and send mode, the first and last bits of the alarm pattern are not significant, in order to avoid any possible errors that may occur due to the technical problems of Send / Receive turnaround or conversely. To prevent repetition of false alarms (noise), the alarm information is only valid when two successive alarms are correctly received
.
The alarms received by a server in repeater mode and from other servers are repeated in the next 8 timeslots (TSlots).

To prevent an echo phenomenon, when the alarm has been repeated, the PLC module will not repeat or transmit any other alarms to the next 9 TSlots.

#### *8.4.1.1.2 Client protocol specification*

The Client profile module must listen continuously for alarm information.

In receive mode, the first and last bits of the alarm pattern are not significant, in order to avoid any possible errors that may occur due to the technical problems of Send / Receive turnaround or conversely. To avoid detecting false alarms caused by noise, the alarm information will be validated when two successive alarms have been correctly received.

In this case, the client physical layer will invoke the P_Alarm.indication service primitive which will be processed by the *System Management AP*.

### 8.4.1.2 CIASE services

#### *8.4.1.2.1 Discover*

*Section deleted in excerpt*

#### *8.4.1.2.2 Clear Alarm Service*

The Clear Alarm Service is used to clear the alarms in the server(s). The service is described in DLMS UA 1000-2 Ed. 7.0.

IDIS supports at least two options for the clear alarm service (comp. DLMS UA 1000-2 Ed. 7.0, sect. 10.4.5.6):

*Section deleted in excerpt*

*Figure 10: The Clear Alarm Service pdu*

##### *8.4.1.2.2.1 Examples for ClearAlarm*

comp. DLMS UA 1000-2 Ed. 7.0, sect 13.3 and considering the IDIS SYSTEM-TITLE-SIZE = 8.

Example 1: Clearing a single alarm in all servers

*Section deleted in excerpt*

Example 2: Clearing a list of alarms in all servers

*Section deleted in excerpt*

Example 3: Clearing a list of alarms in some servers

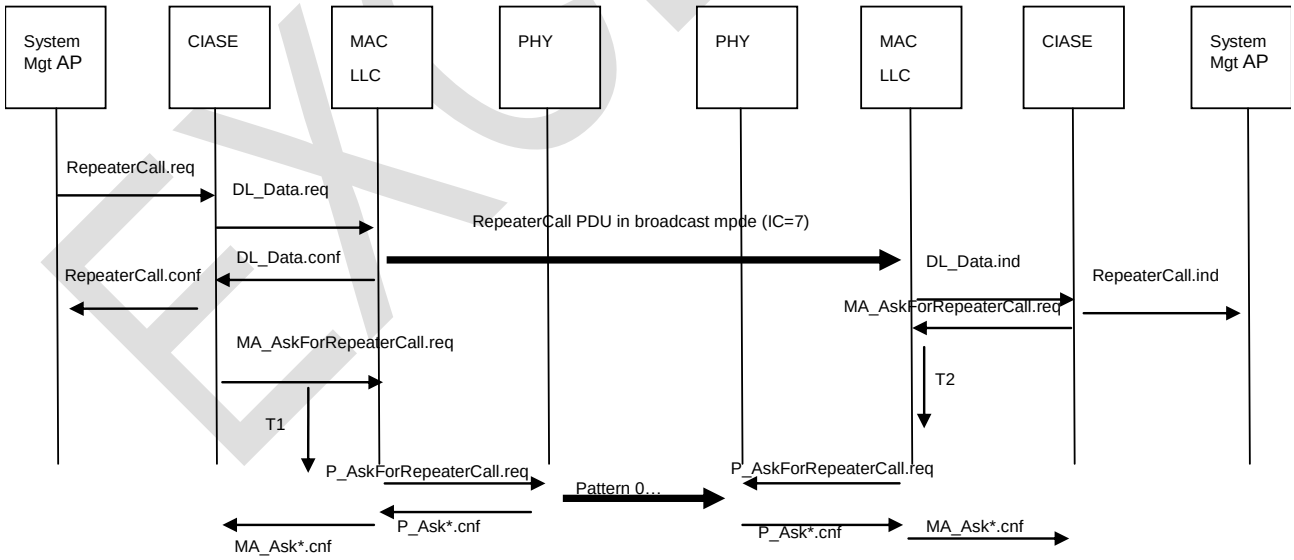
*Section deleted in excerpt*

Example 4: Clearing a different alarm in each different server

*Section deleted in excerpt*

## 8.4.2 Repeater Allocation

IDIS is using the RepeaterCall service specified in section 10.4.5.5 of DLMS UA 1000-2 Ed. 7.0 to automatically configure (as “repeater” or as “no repeater”) those meters which are defined as “dynamic repeaters”. The corresponding parameters are attributes of the COSEM object “S-FSK Phy&MAC setup” with logical_name “0-0:26.0.0.255”. The services involved in the repeater allocation process are displayed in Figure 11.




T1: 8 TSlots (calculated by the MAC layer)

T2: CC * TSlot (calculated by the MAC layer)

*Figure 11 The Repeater allocation services*

### 8.4.2.1 Physical layer services

In *RepeaterCall* mode, the physical layer can no longer see the frames in the usual form. It breaks the PHY frame timeslot (TSlot) down into 21 sub-timeslots (SubTslot) with a duration equivalent to 2 bytes. As the pause time is not used by the RepeaterCall function, the alarms remain active during this period.

*Section deleted in excerpt*

#### *8.4.2.1.1 Client protocol specification*

Upon receiving of the request primitive from the MAC layer, the physical layer in the Client performs the following actions:

*Section deleted in excerpt*

#### *8.4.2.1.2 Server protocol specification*

When a *P_AskForRepeaterCall* request has been received, the physical layer of the server system checks that the arguments are correct and that it is synchronised. If this is not the case, it returns a negative confirmation. Otherwise, it performs the following actions:
For a server in *Dynamic Repeater* mode:

*Section deleted in excerpt*

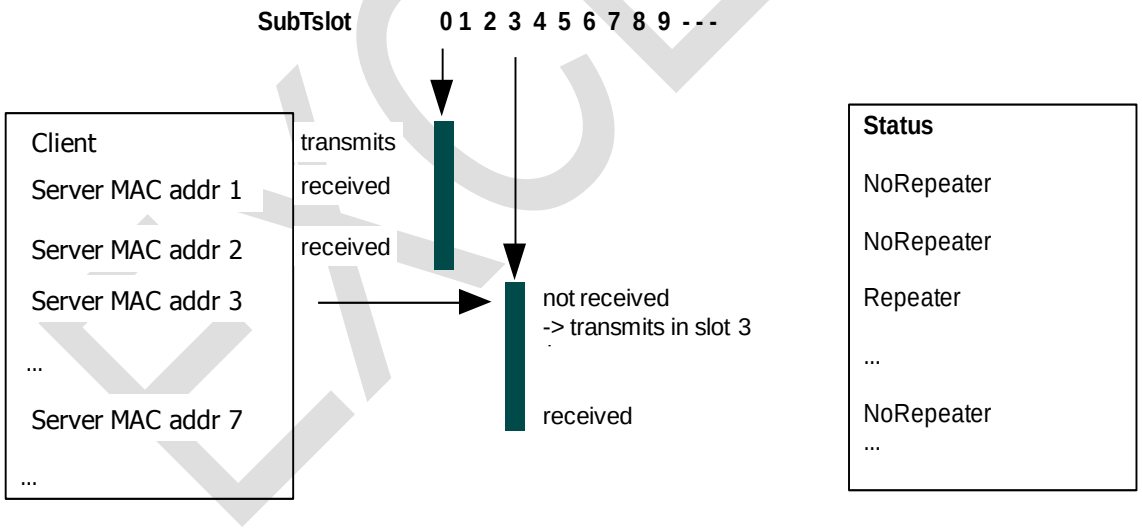



*Figure 12: Server responses to a RepeaterCall*

### 8.4.2.2 MAC layer services

When the MAC layer receives the MA_AskForRepeaterCall.req request, it waits until the physical layer is available to accept the P.AskForRepeaterCall command. The wait time depends on the repetition credit of the current command. (End of repetition wait time = Current Credit * TSlot). It returns a positive confirmation with a result that depends on that returned by the physical layer. If the Repeater Call phase has already begun (end of repetition already reached) when the MAC layer receives the MA_AskForRepeaterCall.req request, the server plays no part in the Repeater Call phase (the P.AskForRepeaterCall command is not invoked). The MAC layer returns a negative confirmation.

## 8.4.3 Initiator allocation

IDIS uses the “Intelligent Search Initiator process” to bind the meter to the concentrator as described in DLMS UA 1000-2 Ed. 7.0, section 10.4.5.7.The objective of the Intelligent Search Initiator process is to improve plug&play installation of the meter, by ensuring that every meter is registered at the correct initiator (concentrator).

*Section deleted in excerpt*

## 8.4.4 Ping Service

The Ping service is allows:

- the concentrator to check that a registered meter is still present in the network;
- to verifying that the right physical device is linked to the right MAC address;
- to prevent the *time_out_not_addressed* timer to expire.

The service primitives are:

- Ping.request (Confirmed service addressed to a server device)
- Ping.confirm
- Ping.indication
- Ping.response

Details are specified in DLMS UA 1000-2 Ed. 7.0 section 10.4.5.1.

### 8.4.4.1 Client service procedure

The Ping.request service primitive is issued by the active initiator.

If the “System_Title_Server” service parameter is not valid, a local confirmation is sent immediately with a negative result indicating the problem encountered (Ping-system-title-nok).

Otherwise, the CIASE forms a DL-Data.request PDU containing a PingRequest CI-PDU that carries the System_Title_Server requested. It is sent to the physical device concerned by the request.

*Section deleted in excerpt*

#### 8.4.4.2 Server service procedure

On the reception of a DL-Data.indication service primitive containing a PingRequest CI-PDU, the CIASE checks that the System_Title_Server service parameter is correct and that it is equal to its own system title.

If so, it invokes a Ping.response service primitive that includes its system title. The PingResponse CI-PDU is carried by a DL-Data.request service primitive.

If the service parameter of the Ping.indication service primitive is not correct, no response is sent. Further, if the System_Title_Server service parameter in the Ping.indication service primitive is correct, but not equal to the system title of the physical device, no response is sent. In both cases the server stays in status “REGISTERED” (comp. sect. 10.4.5.8 in DLMS UA 1000-2 Ed. 7.0).

## 8.5 Management Information Base

The MIB according to IEC 61334-4-512 is accessed via COSEM objects as specified in DLMS UA 1000-1 Ed. 10.0:2010.

*Section deleted in excerpt*

# 9. E-Meter Security Features

IDIS applies the information security methods described in sect. 9.2 of DLMS UA 1000-2 Ed. 7.0.

In IDIS package 1 no dedicated keys are used; i.e. the HES does not need to support the management of the dedicated keys. However, the meters and DC are equipped with all the necessary features to support dedicated keys.

## 9.1 Security setup object

There is only one security setup object through which both the “management association” and the “pre established association” are configured.

| | |
|---|---|
| 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 association and the global broadcast key is related to the pre established association while the authentication key is related to both management association and pre established association. The attributes “security_policy” and the “security_activate” are the same for both associations.

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

*Table 16: relation of the security parameters to the associations*

### 9.1.1.1 Security Setup

For **PLC** communication the *system_title* needed for establishment of the ciphering context (COSEM object security setup, attribute: server_system_title) is automatically stored during registration.

*Section deleted in excerpt*

## 9.1.2 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 (master, dedicated[3], global) per IDIS server.

*Section deleted in excerpt*

The following rules concerning the frame counters apply:

- Framecounters used with dedicated keys are independent of the FCs used with global keys.

*Section deleted in excerpt*

## 9.1.3 Frame counters

Each IDIS server (meter) must store the following frame counters (GET access via public client):

| Key | FC Tx | FC Rx |
|---|---|---|
| Broadcast | na | FCRxb |
| Unicast | FCTxu | FCRxu |

*Table 17: Frame Counters stored in an IDIS server*

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)<br>FCRxb | logical_name: 0-0:43.1.1.255 |
| Security - Receive frame counter - unicast key<br>FCRxu | logical_name: 0-0:43.1.0.255 |

### 9.1.3.1 Re-synchronising the FCs

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

*Section deleted in excerpt*

### 9.1.3.2 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 DC is not aware of the updating of the FC. In this situation the DC must re-synchronise the FCs as defined in 9.1.3.1.

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

## 9.1.4 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. 9.2.4.8.4 of DLMS UA 1000-2 Ed. 7.0.

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.

*Section deleted in excerpt*

### 9.1.4.1 Default passwords and global keys for interoperability testing

For testing propose the following default security material should be used:

*Section deleted in excerpt*

*Table 18 Default values of the security parameters for testing*

NOTE: Each time any of the global keys is changed (by using the master key) the corresponding FC is reset to 0!

## 9.1.5 Putting a meter into field

The following process is performed:

*Section deleted in excerpt*

## 9.1.6 Using Keys

The keys are used as follows:

| Key | Pre-established Client | Management Client | Public Client |
|---|---|---|---|
| Glo-broadcast<br>The same key is used for all meters under one DC.<br>Used with unconfirmed services (invoke_id: bit 6 set to 1). | yes | No | No |
| Glo-unicast<br>A unique key for each meter at least under one DC. | no | Yes | No |
| Glo-authentication<br>The same key is used for all meters under one DC. | yes | Yes | No |
| Ded-unicast<br>A unique key for each meter at least under one DC. | no | yes | no |

*Table 19: Use of the keys*

### 9.1.6.1 Rules to change the Key

*Section deleted in excerpt*

# Index