

Meter Communication Interfaces

Rev.1.0

1 Change Summary

Rev.	Date	Comments
1.0	20.04.2024	Initial document version.

2 Contents

1	Change Summary.....	1
2	Contents	2
3	Introduction.....	3
3.1	Scope of this Document	3
3.2	System Architecture	3
3.3	Acronyms/Definitions	4
4	Communication Profiles	5
4.1	PLC Port.....	5
4.2	Optical Port.....	5
4.3	WAN Port.....	6
5	Logical Devices and Associations	7
5.1	Physical and Logical Devices.....	7
5.2	Minimal Set of Services	7
5.3	The Invoke_Id and Priority Byte.....	7
5.4	Clients.....	7
5.5	Power down.....	12
5.6	Application Association Objects	12
5.7	Handling Associations on Different Ports.....	12
6	Security Features	13
6.1	Security Setup Objects and Security Policies.....	13
6.2	Key Types.....	13
6.2.1	Master Keys.....	13
6.2.2	Global Keys	14
6.2.3	Dedicated Keys.....	15
6.3	Invocation Counters	15
6.3.1	List of Invocation Counters	15
6.3.2	Invocation Counters Storing, Handling and Resetting	15
6.3.3	Re-synchronizing the Invocation Counters	16

3 Introduction

3.1 Scope of this Document

This document provides companion standard for communication interfaces for electricity residential meters.

The goal of the companion standard is to reach an open, standardized protocol implementation based on DLMS/COSEM.

3.2 System Architecture

Electricity meter environment is shown in Fig.1.

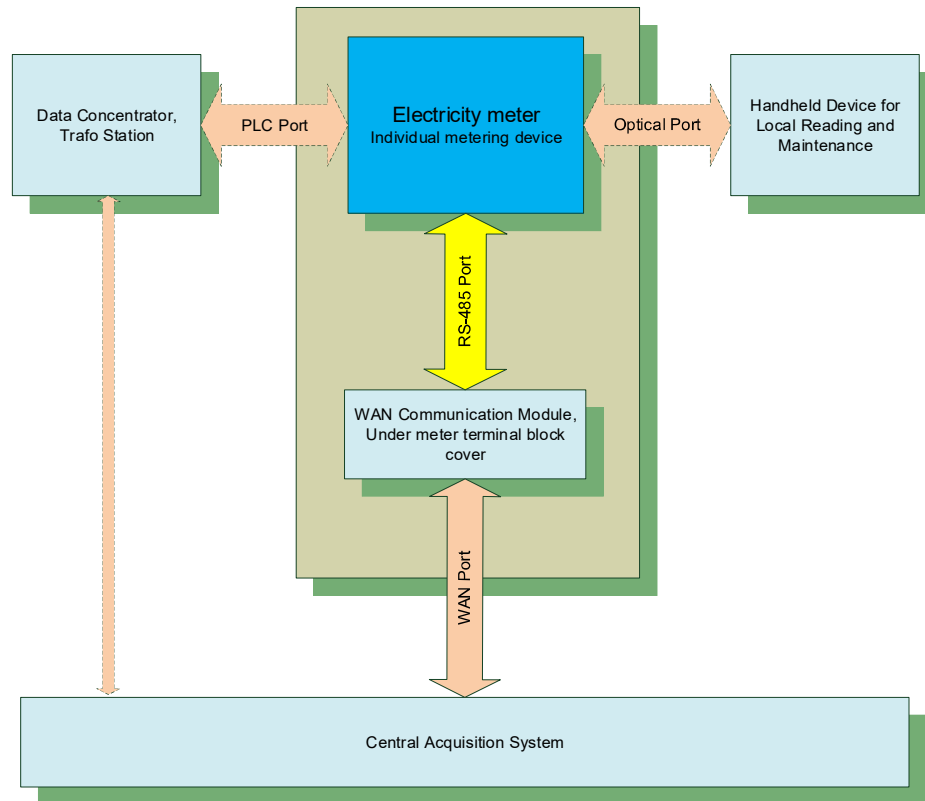


Fig. 1. Meter Interfaces

The communication interfaces shown in dotted lines are out of scope of this document.

All meter interfaces drawn in solid lines are based on the DLMS/COSEM standard. Meter always acts as DLMS/COSEM server, while other entities act as clients. References to the DLMS/COSEM standard are included in text below as footnotes. The companion standard includes only deviations, clarifications or additions to the standard.

Electricity meter has the following physical interfaces:

- PLC Port, designed to communicate with the Data Concentrator, typically mounted at the transformer substation.
- Local Optical Port, designed to communicate with Handheld Unit (Device for Local Reading and Maintenance) or any other compatible equipment.
- Optional WAN Port for communication with the Central Acquisition System (AMI System Central Application) via public 3GPP services.

3.3 Acronyms/Definitions

3GPP – The 3rd Generation Partnership Project (3GPP) is an umbrella term for a number of standards organizations which develop protocols for mobile telecommunications.

AES – Advanced Encryption Standard.

BIT – Broadcast Image Transfer (mechanism of massive remote firmware update).

DB – Database.

DCU – Data Concentrator Unit.

IC – Invocation Counter.

FW – Firmware.

HAN – Home Area Network

HES – Head-End System.

HDLC – High-level Data Link Control

HHU – Hand-Held Unit.

HW – Hardware.

LR&M – Local Reading and Maintenance.

MCU – MicroController Unit.

NRM – Normal Response Mode.

NDM – Normal Disconnected Mode.

PLC – PowerLine Communications

Rx – Receive.

SW – Software.

TS – Transformer Substation.

Tx – Transmit.

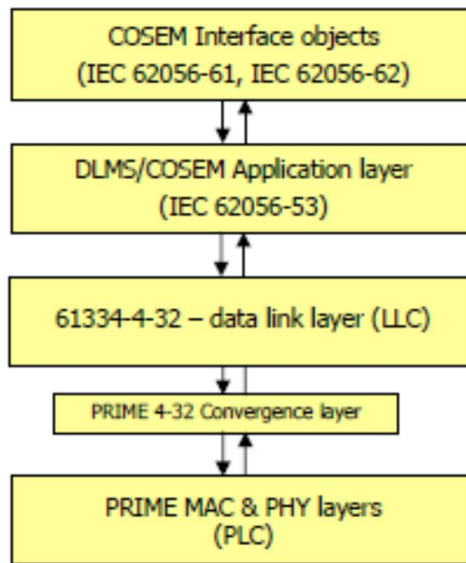
WAN – World Area Network.

4 Communication Profiles

4.1 PLC Port

PRIME low level profile is allowed for the PLC Port. For physical layer, MAC and convergence sub-layers PRIME specification v.1.4 is applicable. By default (factory settings) meter shall operate in PRIME v1.4 Channel #1 (CENELEC A Band), but it shall be possible to switch PRIME modem to Channels #3 to #8.

IEC 61334-4-32 LLC sub-layer is applicable.

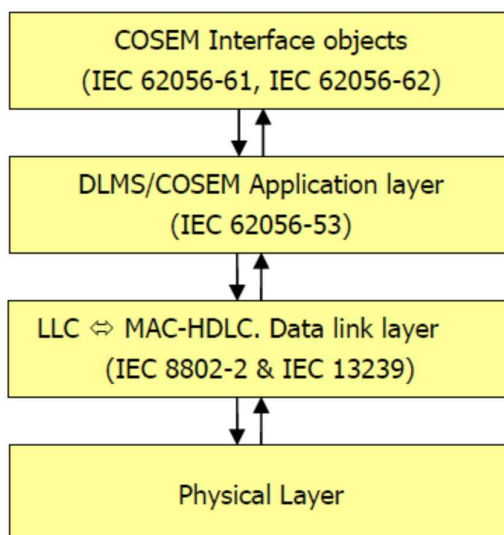


4.2 Optical Port

Physical properties of the optical port shall comply with IEC 62056-21 is applicable. Supported baud rates shall be in the range of 300 to 38400 baud.

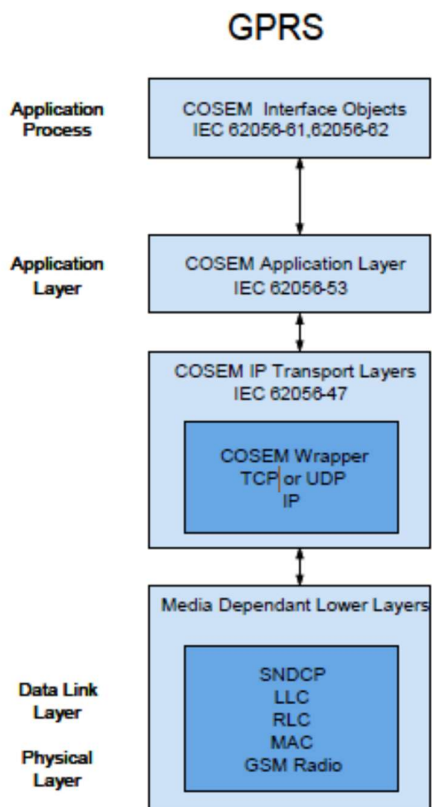
Communication protocol shall be IEC 62056-46.

HDLC addressing scheme: 1 byte for the COSEM Client address and 2 bytes for the COSEM Server address is used. Server lower HDLC address shall be equal to 32 (unconfigurable).



4.3 WAN Port

WAN Port uses TCP/IP COSEM communication profile: 2G 3GPP radio communication network as medium. Transport layer is defined in IEC 62056-4-7.



5 Logical Devices and Associations

5.1 Physical and Logical Devices

In DLMS/COSEM metering equipment normally operated as a COSEM server is modeled in physical and logical devices. In general, actual (physical) device can contain multiple logical devices. For this companion standard physical device can contain only one logical device: the management logical device (L_SAP = 1).

5.2 Minimal Set of Services

Logical Name services are supported. Minimal set of supported application layer services:

- Block-transfer-with-get (11);
- Block-transfer-with-set (12);
- Block-transfer-with-action (13);
- Multiple-references (14);
- Get (19);
- Set (20);
- Selective-Access (21);
- Event-notification (22);
- Action (23).

5.3 The Invoke_Id and Priority Byte

Is handled according to DLMS UA 1000-2 Ed.11.

When the Block Transfer is used to carry long data that do not fit into one APDU, the client must set same Invoke_Id value for all blocks.

Bit 6 (service_class) must be set by the client 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 client, the meter must return the Invoke-Id and Priority byte as received from the client.

5.4 Clients

The following COSEM Clients are permitted by the COSEM server:

- Public Client (L_SAP: 16),
- Reading Client (L_SAP: 2),

- Management Client (L_SAP: 1),
- Firmware Update Client (L_SAP: 3),
- Test Client (L_SAP: 4).

Client	Client L_SAP	Use Cases	Behavior	Services supported by a Server
Public client	16	• Reading basic device configuration information (SAPs, COSEM logical device name, association, serial numbers, etc.). • Unicast communication with the meter.	• Accessible via PLC, Optical and WAN ports. • No security. • Get service only to a limited set of attributes. • Must be established by the 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 inactivity time_out (e.g. TCP/UDP setup object) or on release request.	• Block-transfer-with-get. • Get. • Multiple-references.
Reading Client	2	• Meter parameters reading. • Meter energy register reading.	• Accessible via PLC, Optical and WAN ports. • Must be established by the	• Block-transfer-with-get. • Get. • Multiple-references.

Client	Client L_SAP	Use Cases	Behavior	Services supported by a Server
		Unicast communication with the meter.	- client using the AARQ service with LLS or HLS (mechanism_id(5)). - Supports encryption and authentication. - 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 (e.g. TCP/UDP setup object) or on release request.	- Selective access. - Block-Transfer-with-Action. - Action.
Management Client	1	- Management of the device. - Retrieving data. - Authorized actions in the meter. - Unicast communication with the meter.	- Accessible via PLC, Optical and WAN ports. - Must be established by the client using the AARQ service with LLS or HLS	- Block-transfer-with-get. - Block-transfer-with-set. - Get. - Set. - Multiple-references.

Client	Client L_SAP	Use Cases	Behavior	Services supported by a Server
			(mechanism_id(5)). • Supports encryption and authentication. • 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 (e.g. TCP/UDP setup object) or on release request.	• Selective Access. • Event-notification (transmitted to the PLC or WAN Port). • Block-Transfer-with-Action. • Action.
Firmware Update Client	3	• Firmware update functions. • Unicast and broadcast communication with the meter.	• Accessible via PLC, Optical and WAN ports. • Must be established by the client using the AARQ service with LLS or HLS (mechanism_id(5)).	• Block-transfer-with-get. • Block-transfer-with-set. • Get. • Set. • Multiple-references. • Block-Transfer-with-Action. • Action.

Client	Client L_SAP	Use Cases	Behavior	Services supported by a Server
			• Supports encryption and authentication. • Limited set of access services to a limited set of objects. • 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 (e.g. TCP/UDP setup object) or on release request.	
Test Client	4	• Minimal set of reading functions for inspection and verification purposes.	• Accessible via Optical port only. • Must be established by the client using the AARQ service with LLS or HLS (mechanism_id(5)).	• Get. • Set. • Multiple-references. • Action.

Client	Client L_SAP	Use Cases	Behavior	Services supported by a Server
			• Supports encryption and authentication. • Closing HDLC (optical): on explicit closure, on timeout, on power-down, or on release request.	

Table 1

5.5 Power down

At power down any association opened at the PLC, Optical or WAN ports is closed automatically.

5.6 Application Association Objects

Five Application Association Objects (Association LN, class_id: 15) shall be present in the server: one for each Client.

5.7 Handling Associations on Different Ports

The following rules apply:

- On the Optical Port only one association can be opened at a time.
- On the PLC and WAN Ports several associations may be opened at the same time.
- At different communication ports, only one association with the same client may be opened at the same time.
- Communication ports have different priorities in carrying associations from the same client: the Optical Port has the highest priority, and the PLC Port has the lowest priority. If the same client tries to open additional association on a communication port with higher priority, the server aborts current association and starts opening new association. If the same client tries to open additional association on a communication port with lower priority, the server rejects new association and keeps current association.

6 Security Features

Security architecture is based on the DLMS UA 1000-2 Ed.11¹ concepts. AES-GCM-128 (Galois/Counter Mode with AES-128) Security Suite ID: 0 is implemented for data encryption and authentication and key transport methods.

6.1 Security Setup Objects and Security Policies

Reading, Management, Firmware Update and Test Clients follow their own security policies, configured by separate instances of the Security Setup objects (one for each client).

Each of the following security policies is available:

1. Security is not imposed (default).
2. All messages are encrypted and authenticated.

Management Client is the only one who has rights to configure security policies for all clients, except Firmware Update Client.

Client side is responsible for the harmonization of security policies between different clients.

Security policy can only be strengthened.

6.2 Key Types

Master, global and dedicated keys are used in server.

6.2.1 Master Keys

A master key shall be present in each COSEM Logical Device. This key is used for wrapping global keys.

HES knows master key for each COSEM logical device participating in the system and can change it², invoking `global_key_transfer` method of the Management Security Setup object. New master key is delivered to the meter wrapped by the previous master key. DCU and LR&M device shall not know master keys.

¹ See sub-clause 9.2 for details.

² Secure procedure for master key transport from the manufacturer to HES is out of scope of this document and should be defined and adopted by both sides.

6.2.2 Global Keys

Before ciphering can be used, global keys have to be generated and delivered to the COSEM logical device participating in the system. For delivery, the global keys shall be wrapped by master key using AES-128 wrap algorithm³.

The global keys shall be generated by HES.

The following sets of keys are used:

- A “Reading Key Set” comprised of global unicast encryption key and global authentication key unique for each COSEM logical device is related to the Reading Client association. The “Reading Key Set” shall be made available by HES to LR&M device in a secure way. DCU does not have necessity to know the “Reading Key Set”. The `global_key_transfer` method of the Reading Client Security Setup object shall be invoked by the DCU or LR&M device with the wrapped global key(s) as a parameter.
- A “Management Key Set” comprised of global unicast encryption key and global authentication key unique for each COSEM logical device. The “Management Key Set” shall be made available by HES to DCU (and to LR&M device in case of local communications to the meter) in a secure way. The `global_key_transfer` method of the Management Client Security Setup object shall be invoked then by the DCU or LR&M device with the wrapped global key(s) as a parameter.
- A “Firmware Update Key Set” comprised of global unicast encryption key, global broadcast encryption key and global authentication key unique for each COSEM logical device is related to the Firmware Update Client association. The “Firmware Update Key Set” shall be made available by HES to DCU (and to LR&M device in case of local communications to the meter) in a secure way. The `global_key_transfer` method of the Firmware Update Client Security Setup object shall be invoked then by the DCU or LR&M device with the wrapped global key(s) as a parameter.
- A “Test Key Set” comprised of global unicast encryption key and global authentication key unique for each COSEM logical device. The “Test Key Set” shall be made available by HES to LR&M device in a secure way. The `global_key_transfer` method of the Test Client Security Setup object shall be invoked then by the DCU or LR&M device with the wrapped global key(s) as a parameter.

³ See RFC 3394 for detail.

6.2.3 Dedicated Keys

All associations (except the Public client) should use dedicated keys as a general rule for all associations, and, as a consequence, for all the data transport inside the association.

The dedicated key is established by the DLMS client during the association process.

During decryption and authentication process of the dedicated keys the integrity of the new key must be verified, before activating the new value.

The new values of the keys will be available as soon as they are verified and activated, so they can be used within the current association.

6.3 Invocation Counters

6.3.1 List of Invocation Counters

Each server must store the following Invocation Counters (Tx/Rx directions are considered from server side):

Client	Key	FC Tx	FC Rx
Public Client	n/a	n/a	n/a
Reading Client (RC)	Global unicast	RCICTxu	RCICRxu
	Dedicated	RCICTxd	RCICRxd
Management Client (MC)	Global unicast	MCICTxu	MCICRxu
	Dedicated	MCICTxd	MCICRxd
FW Update Client (FC)	Global unicast	FCICTxu	FCICRxu
	Dedicated	FCICTxd	FCICRxd
	Global broadcast	n/a	FCICRxb
Test Client	Global unicast	TCICTxu	TCICRxu
	Dedicated	TCICTxd	TCICRxd

Table 23

6.3.2 Invocation Counters Storing, Handling and Resetting

Client can access server global FC Rx via Public Client, reading Receive Invocation Counter Unicast and Receive Invocation Counter Broadcast objects (class_id: 1), separate instance per each global FC Rx in the FC Rx column in [Table 2Table-3](#). Dedicated FC Rx are not accessible to the client.

Server must store global FC Rx and FC Tx in the non-volatile memory.

Invocation Counters are handled per client/key type independently of the Communication Port involved in the association.

To avoid counter replay attacks both communicating sides (client and server) must increment corresponding FC for each sent Invocation.

Both sides must validate that each subsequent received Invocation has FC higher than that of the previous one but not more than previous one plus 10 and abort AA immediately when messages are received with FCs not in sequence.

Each time any global key is changed, server resets the corresponding global FC Rx and FC Tx to 0.

Each time the AA is closed, the server destroys the dedicated key and, as a consequence, resets the dedicated FC Rx and FX Tx to 0.

6.3.3 Re-synchronizing the Invocation Counters

Each client re-synchronizes its FCs by reading corresponding server FC Rx values from via Public Client.