Green Book Edition 12

TECHNICAL REPORT

DLMS/COSEM Architecture and Protocols

DLMS UA 1000-2 Ed.12 V1.0
28th May 2025

DLMS User Association

CONTENTS

Foreword

Copyright

This Edition 12 of the Green Book specifies important new elements:

- A new section on attestation public key certificates and infrastructure, 9.2.8;
- A new chapter on attestation and commissioning, 16

In addition, some clarification and editorial changes have been made. See the List of main changes.

This Technical Report is confidential. It may not be copied, nor handed over to persons outside the standardisation environment.

The copyright is enforced by national and international law. The "Berne Convention for the Protection of Literary and Artistic Works" which is signed by 173 countries worldwide and other treaties apply.

Liability

DLMS User Association Publications have the form of recommendations for international use. While all reasonable efforts are made to ensure that the technical content of DLMS User Association Publications is accurate, the DLMS User Association cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

No liability shall attach to DLMS User Association or its directors, employees, servants or agents including individual experts and members of its technical committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this DLMS User Association Publication or any other DLMS User Association Publications.

Acknowledgement

This document has been established by the WG Maintenance of the DLMS UA.

Clause 9.2, Information security in DLMS/COSEM is based on parts of NIST documents. Reprinted courtesy of the National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. Not copyrightable in the United States.

Status of standardisation

The content of Green Book Edition 11 is in line with IEC 62056-5-3:2021 Ed. 4.0, Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer.

To bring the changes in Green Book Edition 12 to international standardisation, updates to IEC 62056-5-3:2021 will be initiated by IEC TC13 WG14.

IEC TC13 WG14 will standardise the mechanisms for attestation and commissioning in the IEC 62056 series.

Revision history

1. Version	Date	Author	Comment
Release 1	1st April 1998	DLMS UA	Initial version
First Edition	1st May 2000	DLMS UA	Major rework, adapted to CDVs of IEC TC13
Second Edition	15th May 2001	DLMS UA	Considering comments to CDVs by IEC National Committees
Third Edition	30th March 2002	DLMS UA	Content adapted to IEC International Standards
Fourth Edition	15th April 2004	DLMS UA	Major rework, adapted to EN and to CDs and NP of IEC TC13 (chapters 4 and 7 are new, change marks added to others)
Fifth Edition	26th August 2005	DLMS-UA	Content aligned with IEC TC 13 CDV-s and comments received.
Sixth Edition	27th August 2007	DLMS UA	Technical content aligned with IEC TC 13 standards published in 2006 / 2007 Document restructured. See list of changes. Sent to WG for approval.
Seventh Edition	22nd December 2009	DLMS UA	Includes: - SN block transfer - Data security - S-FSK PLC profile
Eighth Edition	4th July 2014	DLMS UA	Includes: - Security extensions; - Compression; - ACCESS service; - DataNotification service; - General block transfer mechanism; - XML schema; - Wired and wireless M-Bus profile; - SMS profile; - Gateway protocol; - Compact array encoding example.
Eighth Edition corrected	7th July 2014	DLMS UA	Wrong Figure 139 replaced with the correct one. Missing CIASE APDU module added as 10.5.9.
Edition 8.0 Corrigendum 1	14th December	DLMS UA	Technical and editorial Corrigendum 1 to Edition 8.0.
Edition 8.1	14thth December 2015	DLMS UA	Consolidated edition integrating Corrigendum 1.
Edition 8.2	19th January 2017	DLMS UA	Editorial corrections. Test vector corrections. In line with IEC 62056-5-3 Ed.3.0:2017
Edition 8.3	30th June 2017	DLMS UA	Editorial corrections. Clause added describing the use of the ConfirmedServiceError and ExceptionResponse APDUs. Extended specification of the ExceptionResponse APDU included in Abstract Syntax & XML Schema
Edition 9	8th May 2019	DLMS UA	See below.
Edition 10	31st Auguist 2020	DLMS UA	See below.
Edition 11	21st December 2021	DLMS UA	See below
Edition 12		DLMS UA	See below

List of main technical changes in Edition 9

Item	Clause	Change
1.	9.1.4.4.5	Substantively replaced for clarity. Description of Block Transfer mechanisms
2.	9.1.4.4.9	Substantively replaced for clarity. Description of General Block Transfer.
3.	9.3.2	Inclusion of system title for HLS mechanisms as needed in Calling_AP_Title
4.	9.3.7	Clarification regarding response to SET.request with Attr.0
5.	9.4.6.4	Addition/Correction of response APDU in table 79
6.	9.4.6.13.2	New content clarifying the procedure of operation of the General Block Transfer (GBT)
7.	9.4.6.13.3	New content clarifying the state variables of the General Block Transfer (GBT)
8.	9.4.6.13.4	New content clarifying the stream sub-procedure of the General Block Transfer (GBT)
9.	9.4.6.13.5	New content clarifying the APDU processing sub-procedure of the General Block Transfer (GBT)
10.	9.4.6.13.6	New content clarifying the retry sub-procedure of the General Block Transfer (GBT)
11.	9.4.6.14	Paragraph moved for clarity
12.	12.2	Clarification of the example in Table 141
13.	C.1	Additions of brackets to key agreement data for clarity to Figure C.1
14.	C.2	Addition of bracket to key-info data for clarity to Figure C.2

List of main technical changes in Edition 10

Item	Clause	Change
1.	9.1.4.3.1	Push added
2.	9.3.10	Text changed to add reliable push
3.	9.4.6.2.2	New clause for push services
4.	9.4.6.7	New description and figures for the reliable push
5.	9.5	Delta types added, syntax added for confirm push
6.	9.6	Delta types added, XML Schema added for confirm push
7.	10.8	New profile for LPWAN
8.	10.9	New profile added for Wi-SUN
9.	14.4	Profile generic IC buffer attribute encoding examples using various encoding techniques added
10.	Figure 5	Confirmed DataNotification service added to Figure
11.	Figure 88	Push added
12.	Figure 90	Push added
13.	Figure 91	Push added
14.	Figure 116	Notification services added for reliable push
15.	Figure 117	Notification services added for reliable push
16.	Table 76	.response and .confirm parameters added
17.	Table 89	Add services for reliable push

List of main technical changes in Edition 11

Item	Clause	Change
1.	9.3.10	Data notification service modifies to support CoAP reliable and unreliable push
2.	10.4	New clause covering the CoAP profile. Further modifications in clauses 4.8, and 7 to support CoAP
3.	7.3.6	New clause to support CoAP.
4.		

List of main technical changes in Edition 12

Item	Clause	Change
1.	9.1.4.4.3	Added clarification on behaviour in the case of the unsolicited DataNotification.request (from Contribution 125)
2.	9.2.8	New section on attestation public key certificates and infrastructure (from Contribution 109)
3.	16	New chapter on attestation and commissioning (from Contribution 109)
4.		
5.		
6.		
7.		
8.		

1 Scope

The DLMS/COSEM specification specifies an interface model and communication protocols for data exchange with connected devices.

The interface model provides a view of the functionality of the device as it is available at its interface(s). It uses generic building blocks to model this functionality. The model does not cover internal, implementation-specific issues.

Communication protocols define how the data can be accessed and transported.

The DLMS/COSEM specification follows a three-step approach as illustrated in

Figure 1:

- Step 1, Modelling: This covers the interface model of a device and rules for data identification;
- Step 2, Messaging: This covers the services for mapping the interface model to protocol data units (APDU) and the encoding of this APDUs.
- Step 3, Transporting: This covers the transportation of the messages through the communication channel.

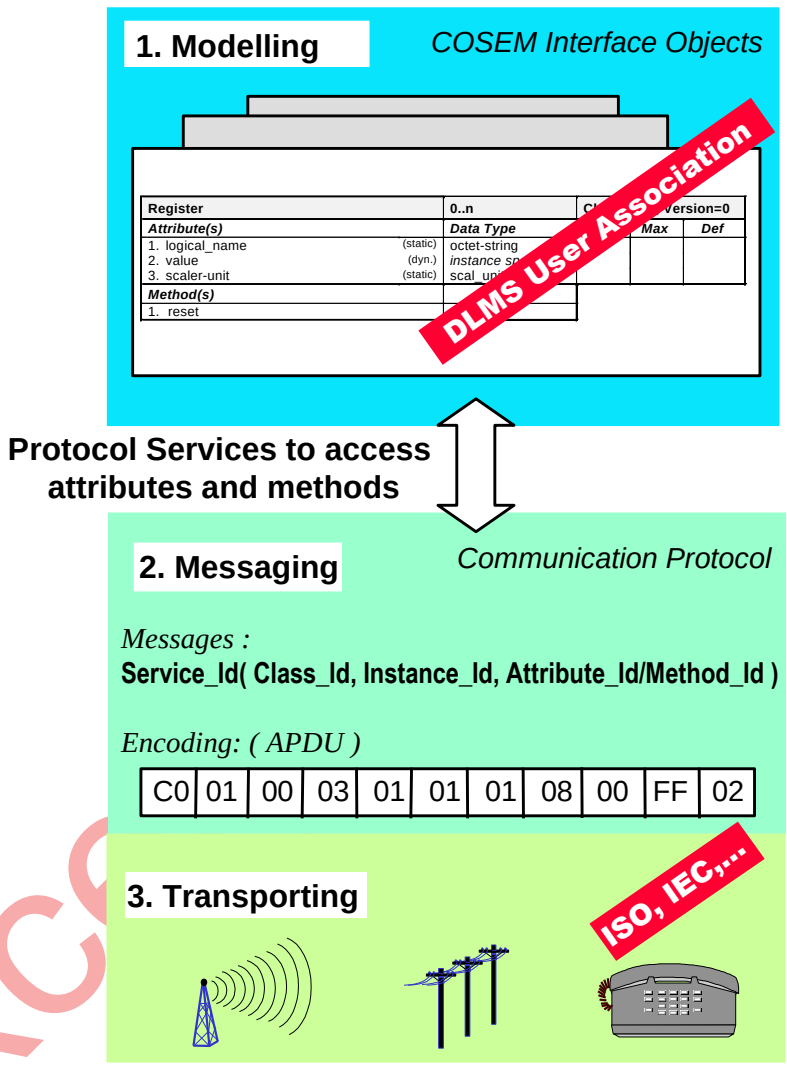

Figure 1 – The three steps approach of COSEM: Modelling – Messaging – Transporting

Step 1 is specified in the document "COSEM interface classes and the OBIS identification system" DLMS UA 1000-1. It specifies the COSEM interface classes, the OBIS identification system used to identify instances of these classes, called interface objects, and the use of interface objects for modelling the various functions of the device.

Step 2 and 3 are specified in this Technical Report.

The DLMS/COSEM application layer (AL) specifies the services to establish logical connections between a client and (a) server(s) and the services to access attributes and methods of the COSEM objects. The DLMS/COSEM AL is specified in Clause 9.

DLMS/COSEM communication media specific profiles specify how application layer messages can be transported over various communication media. Each communication profile specifies the set of the protocol layers required to support the DLMS/COSEM AL on top. See also 4.8.

Large scale deployment of smart connected systems requires strong information security mechanisms to protect the privacy of consumers, the business interests of the service providers and the security of the infrastructure.

DLMS/COSEM provides built-in security mechanisms from the outset. Initially, it provided mechanisms for the identification and authentication of clients and servers, as well as specific access rights to COSEM object attributes and methods within application associations (AAs) established between a client and a server. Ciphered APDUs were also available to allow protecting the messages exchanged between clients and servers.

In the next step, the details of ciphering using symmetric key algorithms, providing authentication and encryption as well as key transport mechanisms have been specified.

Rules for conformance testing are specified in the document DLMS UA 1001-1 "DLMS/COSEM Conformance Test Process".

Terms are explained in Clause 3 and in DLMS UA 1002 "COSEM Glossary of Terms".

2 Normative references

Ref.	Title
DLMS UA 1000-1 Part 2 Ed.17:2025	COSEM Interface Classes and OBIS Identification System, the “Blue Book”
DLMS UA 1000-1 Part 1	COSEM Interface Classes and OBIS Identification System, the “Blue Book” NOTE This undated reference is used unless a specific clause needs to be referenced.
DLMS UA 1001-1	DLMS/COSEM Conformance test and certification process, the “Yellow Book”
DLMS UA 1002 Ed. 1.0:2003	COSEM Glossary of Terms, "White Book"
IEC 61334-4-1:1996	Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 1: Reference model of the communication system
IEC 61334-4-32:1996	Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 32: Data link layer – Logical link control (LLC)
IEC 61334-4-41:1996	Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocol – Distribution line message specification
IEC 61334-4-511:2000	Distribution automation using distribution line carrier systems – Part 4-511: Data communication protocols – Systems management – CIASE protocol
IEC 61334-5-1:2001	Distribution automation using distribution line carrier systems – Part 5-1: Lower layer profiles – The spread frequency shift keying (S-FSK) profile
IEC 61334-6:2000	Distribution automation using distribution line carrier systems – Part 6: A-XDR encoding rule
IEC 62056-1-0	Electricity metering data exchange – The DLMS/COSEM suite – Part 1 0: Smart metering standardisation framework
IEC 62056-21:2002	Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange
IEC 62056-8-20:2016	Electricity metering data exchange - The DLMS/COSEM suite - Part 8-20: Mesh communication profile for neighbourhood networks
ISO/IEC 7498-1:1994	Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model
ISO/IEC 8649 Ed. 2.0:1996	Information technology – Open Systems Interconnection – Service definition for the Association Control Service Element NOTE This standard has been replaced by ISO/IEC 15953:1999
ISO/IEC 8650-1 Ed 2.0:1996	Information technology – Open systems interconnection – Connection-oriented protocol for the association control service element: Protocol specification NOTE This standard has been replaced by ISO/IEC 15954:1999
ISO/IEC 8802-2 Ed. 3.0:1998	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control
ISO/IEC 8824:2008	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation
ISO/IEC 8825-1:2015	Information technology - ASN.1 encoding rules: Specification of : Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
ISO/IEC 13239:2002	Information Technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures
ISO/IEC 15953:1999	Information technology — Open Systems Interconnection — Service definition for the Application Service Object Association Control Service Element NOTE This standard cancels and replaces ISO/IEC 8649:1996 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.
ISO/IEC 15954:1999	Information technology — Open Systems Interconnection — Connection-mode protocol for the Application Service Object Association Control Service Element

	NOTE This standard cancels and replaces ISO/IEC 8650-1:1999 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.
EN13757-1:2014	Communication system for and remote reading of meters – Part 1: Data exchange
EN 13757-2:2004	Communication system for and remote reading of meters – Part 2 : Physical and Link Layer, Twisted Pair Baseband (M-Bus)
EN 13757-3:2018	Communication systems for meters - Part 3: Application protocols
EN 13757-4:2013	Communication system for and remote reading of meters – Part 4: Wireless meter (Radio meter reading for operation in SRD bands)
EN 13757-5:2015	Communication system for and remote reading of meters – Part 5: Wireless relaying
EN 13757-6:2015	Communication system for meters – Part 6: Local Bus
EN 13757-7:2018	Communication systems for meters - Part 7: Transport and security services
ETSI-TS-102-887-2	Electromagnetic compatibilityand Radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol; Part 2: Data Link Layer (MAC Sub-layer)
IEEE 802.1ar	IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity, IEEE Std 802.1AR-2009
IEEE 802.1X	IEEE Standard for Local and Metropolitan Area Networks – Port Based Network Access Control", IEEE Std 802.1X-2010
IEEE 802.11i	IEEE Standard for Information Technology— Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications IEEE Std 802.11-2012 NOTE the 802.11i amendment was specifically for the inclusion of Wi-Fi Protected Access (WPA 2) security which is the part that is relevant to this standard.
IEEE 802.15.4	IEEE Standard for Low-Rate Wireless Networks
ITU-T V.44: 2000	SERIES V: DATA COMMUNICATION OVER THE TELEPHONE NETWORK – Error control – V.44:2000, Data compression procedures
ITU-T X.211	SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY – Information technology – Open systems interconnection – Physical Service Definition
ITU-T X.509:2008	SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY – Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks
ITU-T X.693 (11/2008)	Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)
ITU-T X.693 Corrigendum 1(10/2011)	Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1
ITU-T X.694 (11/2008)	Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1
ITU-T X.694 Corrigendum 1 (10/2011)	Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1Technical Corrigendum 1
ANSI C12.21:1999	Protocol Specification for Telephone Modem Communication
FIPS PUB 180-4:2012	Secure Hash Standard (SHS)
FIPS PUB 186-4:2013	Digital Signature Standard (DSS)
FIPS PUB 197:2001	Advanced Encryption Standard (AES)
LoRaWAN Spec 1.0.3	https://lora-alliance.org/resource-hub/lorawanr-specification-v103.
NIST SP 800-21:2005	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-32:2001	Introduction to Public Key Technology and the Federal PKI Infrastructure
NIST SP 800-38D:2007	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
NIST SP 800-56A Rev. 2: 2013	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
NIST SP 800-57:2012	Recommendation for Key Management – Part 1: General (Revision 3)
NSA1	Suite B Implementer's Guide to FIPS 186-3 (ECDSA), Feb 3rd 2010

NSA2	Suite B Implementer's Guide to NIST SP800-56A, 28th July 2009
NSA3	NSA Suite B Base Certificate and CRL Profile, 27th May 2008
[FANSPEC]	Wi-SUN Alliance: Field Area Network Working Group (FANWG):Technical Profile Specification:Field Area Network:Version 1v26.
[PHYSPEC]	Wi-SUN Alliance: PHY Working Group (PHYWG) Wi-SUN PHY Specification Revision 1V02
ANSI/TIA-4957.200	Layer 2 Standard Specification for the Smart Utility Network
ANSI/TIA 4957.210	Multi-Hop Sublayer Specification-Extension on Field Area Networks
The following RFCs are available on line from the Internet Enegineering Task Force (IETF): https://www.ietf.org/rfc/std-index.txt, https://www.ietf.org/rfc/	
RFC 768	User Datagram Protocol
RFC 793	Transmission Control Protcol
RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 2460	Internet Protocol, Version 6
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3394	Advanced Encryption Standard (AES) Key Wrap Algorithm, 2002
RFC 4108	Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages, 2005
RFC 4291	IP Version 6 Addressing Architecture
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
RFC 5216	The EAP-TLS Authentication Protocol
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6206	The Trickle Algorithm
RFC 6282	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks
RFC 6550	RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks
RFC 6775	Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks 409 (6LoWPANs)
RFC 7217	A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC). Edited by F. Gont.
RFC 7731	Multicast Protocol for Low-Power and Lossy Networks (MPL)
RFC 7252	The Constrained Application Protocol.
RFC 7774	Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6
RFC 7959	Block-Wise Transfers in the Constrained Application Protocol (CoAP)
RFC 8376	Low-Power Wide Area Network (LPWAN) Overview. Edited by S. Farrell, May 2018.
RFC 8724	SCHC – Generic Framework for Static Context Header Compression and Fragmentation. April 2020.
IETF Internet Draft	Static Context Header Compression (SCHC) over LoRaWAN.
STD0005 (1981)	Internet Protocol. Also: RFC0791, RFC0792, RFC0919, RFC0922, RFC0950, RFC1112
STD0006 (1980)	User Datagram Protocol. Also: RFC0768
STD0007 (1981)	Transmission Control Protocol. Also: RFC0793

3 Terms, definitions and abbreviations and symbols

3.1 General DLMS/COSEM definitions

3.1.1

ACSE APDU
APDU used by the Association Control Service Element (ACSE)

3.1.2

application association
cooperative relationship between two application entities, formed by their exchange of application protocol control information through their use of presentation services

3.1.3

application context
set of application service elements, related options and any other information necessary for the interworking of application entities in an application association

3.1.4

application entity
the system-independent application activities that are made available as application services to the application agent, e.g., a set of application service elements that together perform all or part of the communication aspects of an application process

3.1.5

application process
an element within a real open system which performs the information processing for a particular application

[SOURCE: ISO/IEC 7498-1:1994, 4.1.4]

3.1.6

authentication mechanism
the specification of a specific set of authentication-function rules for defining, processing, and transferring authentication-values

[SOURCE: ISO/IEC 15953:1999, 3.5.11]

3.1.7

block

one portion of an xDLMS APDU; the payload of a GBT APDU

3.1.8

client
application process running in the data collection system

3.1.9

client/server
relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request

3.1.10

confirmed GBT procedure
procedure in which the sender sends streams of GBT APDUs and at the end of each stream the recipient acknowledges the blocks received and attempts recovering any missing blocks

Note 1 to entry: A GBT stream consists of one or more GBT APDUs.

Note 2 to entry: In the case of a confirmed GBT stream the end of the stream is indicated by the streaming bit to set to FALSE (0). In the case of an unconfirmed GBT stream the end of the stream is indicated by the Final bit set to TRUE (1).

3.1.11

COSEM
Comprehensive Semantic Model for Energy Management; refers to the COSEM object model

3.1.12

COSEM APDU
comprises ACSE APDUs and xDLMS APDUs

3.1.13

COSEM data
COSEM object attribute values, method invocation and return parameters

3.1.14

COSEM interface class
entity with specific set of attributes and methods modelling a certain function on its own or in relation with other COSEM interface classes

3.1.15

COSEM object
instance of a COSEM interface class

3.1.16

DLMS/COSEM
refers to the application layer providing xDLMS services to access COSEM interface object attributes. Also refers to the DLMS/COSEM Application layer and the COSEM data model together.

3.1.17

DLMS context
a specification of the service elements of DLMS and semantics of communication to be used during the lifetime of an application association

[SOURCE: IEC 61334-4-41:1996, 3.3.5]

3.1.18

entity authentication
corroboration that an entity is the one claimed

[SOURCE: ISO/IEC 9798-1:2010, 3.14]

3.1.19

gap
empty space i.e. missing blocks in the receive queue RQ

Note to entry: A receive queue RQ may have one or more gaps. In each gap, one or more blocks may be missing.

3.1.20

GBT APDU
xDLMS APDU with control information that carries a block of another xDLMS APDU or an empty block

3.1.21

GBT exchange
exchanging GBT APDUs that carry the service primitives of the same service

3.1.22

GBT stream
a sequence of GBT APDUs

3.1.23

general block transfer
GBT
DLMS/COSEM application layer mechanism that can transfer any other xDLMS APDU that would be otherwise too long to fit into the maximum APDU size negotiated, in several blocks.

Note to entry: GBT can be forced by including GBT parameters in the .request service primitive.

3.1.24

logical device
abstract entity within a physical device, representing a subset of the functionality modelled with COSEM objects

3.1.25

master
central station – station which takes the initiative and controls the data flow

3.1.26

message
xDLMS APDU carrying a service primitive in an encoded form, which may also be cryptographically protected

3.1.27

mutual authentication
entity authentication which provides both entities with assurance of each other's identity

Note to entry: The DLMS/COSEM HLS authentication mechanism provides mutual authentication.

[SOURCE: ISO/IEC 9798-1:2010, 3.18 modified by adding Note 1]

3.1.28

overflow
more GBT APDUs received in one stream than the size of the GBT window

3.1.29

physical device
the highest level element used in the COSEM interface model of devices

3.1.30

pull operation
style of communication where the request for a given transaction is initiated by the client

3.1.31

push operation
style of communication where the request for a given transaction is initiated by the server

3.1.32

receive queue
RQ
placeholder for the blocks of the APDU received in a GBT stream

3.1.33

server
an application process running in a device

3.1.34

send queue
SQ
placeholder for the blocks of the APDU to be sent

3.1.35

service-specific block transfer
DLMS/COSEM application layer mechanism that can transfer an xDLMS APDU corresponding to a specific service primitive, that would be otherwise too long to fit into the maximum APDU size negotiated, in several blocks

3.1.36

streaming window
number of GBT APDUs that can be received in a stream

3.1.37

slave
station responding to requests of a master station.

Note to entry: A device is normally a slave station.

3.1.38

system title
unique identifier of the system

3.1.39

unconfirmed GBT procedure
procedure in which the sender sends and the recipient receives a single stream of GBT APDUs, the recipient does not acknowledge the blocks received and does not attempt to recover any blocks lost

Note to entry: This is used to carry unconfirmed service requests from the client to the server or unsolicited service requests from the server to the client.

3.1.40

unilateral authentication
entity authentication which provides one entity with assurance of the other's identity but not vice versa

Note to entry: The DLMS/COSEM LLS authentication mechanism provides unilateral authentication.

[SOURCE: ISO/IEC 9798-1:2010, 3.39]

3.1.41

xDLMS
extended DLMS; refers to the DLMS protocol with the extensions specified in this Technical Report

3.1.42

xDLMS APDU
APDU used by the xDLMS Application Service Element (xDLMS ASE)

3.1.43

xDLMS message
xDLMS APDU exchanged between a client and a server or between a third party and a server

3.2 Definitions related to cryptographic security

3.2.1

access control
restricts access to resources to only privileged entities.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.2

asymmetric key algorithm
see Public key cryptographic algorithm

3.2.3

authentication
a process that establishes the source of information, provides assurance of an entity's identity or provides assurance of the integrity of communications sessions, messages, documents or stored data.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.4

authentication code
a cryptographic checksum based on an approved security function (also known as a Message Authentication Code)

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.5

certificate
see public key certificate

3.2.6

Certification Authority
CA
the entity in a Public Key Infrastructure (PKI) that is responsible for issuing public key certificates and exacting compliance to a PKI policy

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.7

Certificate Policy
CP
a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

[SOURCE: NIST SP 800-32:2001]

3.2.8

challenge
a time variant parameter generated by a verifier

[SOURCE: ITU-T X.811:1995, 3.8]

3.2.9

ciphering
authentication and / or encryption using symmetric key algorithms

3.2.10

ciphertext
data in its encrypted form

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.11

cofactor
the order of the elliptic curve group divided by the (prime) order of the generator point (i.e. the base point) specified in the domain parameters

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.12

confidentiality
the property that sensitive information is not disclosed to unauthorized entities

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.13

cryptographic algorithm
a well-defined computational procedure that takes variable inputs including a cryptographic key and produces an output

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.14

cryptographic key
key
a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot

Note to entry:

Examples include:

1. The transformation of plaintext data into ciphertext data,
2. The transformation of ciphertext data into plaintext data,
3. The computation of a digital signature from data,
4. The verification of a digital signature,
5. The computation of an authentication code from data,
6. The verification of an authentication code from data and a received authentication code,
7. The computation of a shared secret that is used to derive keying material.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.15

cryptoperiod
the time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.16

dedicated key
in DLMS/COSEM, a symmetric key used within a single instance of an Application Association. See also session key

3.2.17

deprecated
not recommended for new implementations

3.2.18

digital signature
the result of a cryptographic transformation of data that, when properly implemented with supporting infrastructure and policy, provides the services of:

1. origin authentication

2. data integrity, and

3. signer non-repudiation

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.19

directly trusted CA
a directly trusted CA is a CA whose public key has been obtained and is being stored by an end entity in a secure, trusted manner, and whose public key is accepted by that end entity in the context of one or more applications

[SOURCE: ISO/IEC 15945:2002, 3.4]

3.2.20

directly trusted CA key
a directly trusted CA key is a public key of a directly trusted CA. It has been obtained and is being stored by an end entity in a secure, trusted manner. It is used to verify certificates without being itself verified by means of a certificate created by another CA.

Note to entry: Directly trusted CAs and directly trusted CA keys may vary from entity to entity. An entity may regard several CAs as directly trusted CAs.

[SOURCE: ISO/IEC 15945:2002, 3.5]

3.2.21

distribution
see key distribution

3.2.22

domain parameters
the parameters used with a cryptographic algorithm that are common to a domain of users

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.23

encryption
the process of changing plaintext into ciphertext using a cryptographic algorithm and key

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.24

ephemeral key
a cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message or session). In some cases ephemeral keys are used more than once, within a single “session (e.g., broadcast applications) where the sender generates only one ephemeral key pair per message and the private key is combined separately with each recipient’s public key.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.25

global key
a key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a DLMS/COSEM Application Association, see also static symmetric key

3.2.26

hash function
a function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1) One-way: It is computationally infeasible to find any input that maps to any pre-specified output, and

2) Collision resistant: It is computationally infeasible to find any two distinct inputs that map to the same output.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.27

hash value
the result of applying a hash function to information

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.28

initialization vector
IV
a vector used in defining the starting point of a cryptographic process

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.29

identification
the process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system

[SOURCE: NIST SP 800-47:2002]

3.2.30

key
see cryptographic key

3.2.31

key agreement
a (pair-wise) key-establishment procedure in which the resultant secret keying material is a function of information contributed by both participants, so that neither party can predetermine the value of the secret keying material independently from the contributions of the other party. Contrast with key-transport.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.32

key-confirmation
a procedure to provide assurance to one party (the key-confirmation recipient) that another party (the key-confirmation provider) actually possesses the correct secret keying material and/or shared secret

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.33

key-derivation function
a function by which keying material is derived from a shared secret (or a key) and other information

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.34

key distribution
the transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.35

key-encrypting key
a cryptographic key that is used for the encryption or decryption of other keys

Note to entry: In DLMS/COSEM it is the master key.

[SOURCE: NIST SP 800-57:2012 Part 1, modified by adding the Note]

3.2.36

key establishment
the procedure that results in keying material that is shared among different parties

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.37

key pair
a public key and its corresponding private key; a key pair is used with a public key algorithm

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.38

key revocation
a function in the lifecycle of keying material; a process whereby a notice is made available to affected entities that keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.39

key-transport
a (pair-wise) key-establishment procedure whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Contrast with key agreement.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.40

key wrapping
a method of encrypting keying material (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.41

message authentication code
MAC
a cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.42

message digest
the result of applying a hash function to a message. Also known as “hash value”.

[SOURCE: FIPS PUB 186-4:2013]

3.2.43

named curve
a set of ECDH domain parameters is also known as a "curve". A curve is a "named curve" if the domain parameters are well known and defined and can be identified by an Object Identifier; otherwise, it is called a "custom curve".

[SOURCE: RFC 5349]

3.2.44

nonce
a time-varying value that has at most an acceptably small chance of repeating. For example, the nonce may be a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.45

non-repudiation
a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the claimed signatory

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.46

password
a string of characters (letters, numbers and other symbols) that are used to authenticate an identity or to verify access authorization or to derive cryptographic keys.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.47

plaintext
intelligible data that has meaning and can be understood without the application of decryption

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.48

private key
a cryptographic key, used with a public key cryptographic algorithm, which is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to:

1) Compute the corresponding public key,

2) Compute a digital signature that may be verified by the corresponding public key,

3) Decrypt keys that were encrypted by the corresponding public key, or

4) Compute a shared secret during a key-agreement transaction.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.49

protected
ciphered and /or digitally signed. Protection may be applied to xDLMS APDUs and/or to COSEM data.

3.2.50

public key
a cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used, for example, to:

1) Verify a digital signature that is signed by the corresponding private key,

2) Encrypt keys that can be decrypted using the corresponding private key, or

3) Compute a shared secret during a key-agreement transaction.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.51

public-key certificate
a data structure that contains an entity's identifier(s), the entity's public key (including an indication of the associated set of domain parameters) and possibly other information, along with a signature on that data set that is generated by a trusted party, i.e. a certificate authority, thereby binding the public key to the included identifier(s).

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.52

public key (asymmetric) cryptographic algorithm
a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that determining the private key from the public key is computationally infeasible.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.53

Public Key Infrastructure
PKI
a framework that is established to issue, maintain and revoke public key certificates.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.54

receiver <key-transport>
the party that receives secret keying material via a key-transport transaction. Contrast with sender.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.55

revoke a certificate
to prematurely end the operational period of a certificate effective at a specific date and time

[SOURCE: NIST SP 800-32:2001]

3.2.56

Root Certification Authority
in a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain

[SOURCE: NIST SP 800-32:2001]

3.2.57

secret key
a cryptographic key that is used with a secret key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.58

security services
mechanisms used to provide confidentiality, data integrity, authentication or non-repudiation of information

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.59

security strength
(also “bits of security”)
a number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.60

self-signed certificate
a public key certificate whose digital signature may be verified by the public key contained within the certificate. The signature on a self-signed certificate protects the integrity of the data, but does not guarantee authenticity of the information. The trust of self-signed certificates is based on the secure procedures used to distribute them.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.61

sender <key-transport>
the party that sends secret keying material to the receiver in a key-transport transaction. Contrast with receiver.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.62

session key
cryptographic key established for use for a relatively short period of time. In DLMS/COSEM the dedicated key is a session key.

3.2.63

shared secret
a secret value that has been computed using a key agreement scheme and is used as input to a key-derivation function/method

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.64

signature generation
uses a digital signature algorithm and a private key to generate a digital signature on data

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.65

signature verification
uses a digital signature algorithm and a public key to verify a digital signature on data

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.66

signed data
data upon which a digital signature has been computed

3.2.67

static symmetric key
key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a DLMS/COSEM Application Association

Note to entry: In DLMS/COSEM it is known as global key.

3.2.68

static key
a key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establishment scheme. Contrast with an ephemeral key.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.69

Subordinate Certification Authority
in a hierarchical PKI, a Certification Authority (CA) whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA

[SOURCE: NIST SP 800-32:2001]

3.2.70

symmetric key
a single cryptographic key that is used with a secret (symmetric) key algorithm

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.71

symmetric key algorithm
a cryptographic algorithm that uses the same secret key for an operation and its complement (e.g., encryption and decryption)

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.72

trust anchor
a public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.73

trusted party
a trusted party is a party that is trusted by an entity to faithfully perform certain services for that entity. An entity could be a trusted party for itself.

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.74

trusted third party
a third party, such as a CA, that is trusted by its clients to perform certain services. (By contrast, in a key establishment transaction, the participants, parties U and V, are considered to be the first and second parties.)

[SOURCE: NIST SP 800-56A Rev. 2: 2013]

3.2.75

X.509 certificate
the X.509 public-key certificate or the X.509 attribute certificate, as defined by the ISO/ITU-T X.509 standard. Most commonly (including in this document), an X.509 certificate refers to the X.509 public-key certificate.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.2.76

X.509 public key certificate

a digital certificate containing a public key for entity and a name for the entity, together with some other information that is rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.

[SOURCE: NIST SP 800-57:2012, Part 1]

3.3 Definitions and abbreviations related to the Galois/Counter Mode

The source of the definitions 3.3.1 to 3.3.13 abbreviations and symbols in this subclause is NIST SP 800-38D:2007.

3.3.1

Additional Authenticated Data
AAD
input data to the authenticated encryption function that is authenticated but not encrypted

3.3.2

authenticated decryption
function of GCM in which the ciphertext is decrypted into the plaintext, and the authenticity of the ciphertext and the AAD are verified

3.3.3

authenticated encryption
function of GCM in which the plaintext is encrypted into the ciphertext and an authentication tag is generated on the AAD and the ciphertext

3.3.4

authentication tag
Tag, T
cryptographic checksum on data that is designed to reveal both accidental errors and the intentional modification of the data

3.3.5

block cipher
parameterized family of permutations on bit strings of a fixed length; the parameter that determines the permutation is a bit string called the key

3.3.6

ciphertext
encrypted form of the plaintext

3.3.7

fixed field
in the deterministic construction of IVs, the field that identifies the device or context for the instance of the authenticated encryption function

3.3.8

fresh
for a newly generated key, the property of being unequal to any previously used key

3.3.9

GCM
Galois/Counter Mode

3.3.10

initialization Vector
IV
nonce that is associated with an invocation of authenticated encryption on a particular plaintext and AAD

Note to entry: For the purposes of this standard, the invocation field is the invocation counter.

3.3.11

invocation field
in the deterministic construction of IVs, the field that identifies the sets of inputs to the authenticated encryption function in a particular device or context

3.3.12

key
parameter of the block cipher that determines the selection of the forward cipher function from the family of permutations

3.3.13

plaintext
P
input data to the authenticated encryption function that is both authenticated and encrypted

3.3.14

security control byte
SC
byte that provides information on the ciphering applied

3.3.15

security header
SH
concatenation of the security control byte SC and the invocation counter: $SH = SC \text{ II } IC$.

3.4 Definitions and abbreviations related to Wi-SUN

3.4.1

border router node
device that acts as the control point for multiple router devices across a large network

3.4.2

leaf node
device that does not provide any routing capability

3.4.3

operating class
with regulatory domain, reference to regionally allowable frequency bands

NOTE to entry: Regulatory Domains and frequency bands are defined in [FANSPEC].

3.4.4

Personal Area Network (PAN)
network area subservient to a border router node

3.4.5

regulatory domain
with operating class, reference to regionally allowable frequency bands

NOTE to entry: Regulatory Domains and frequency bands are defined in [FANSPEC]

3.4.6

router/forwarding node
device that manages messages between end nodes and the border router

3.5 General abbreviations

Abbreviation	Meaning
.cnf	.confirm service primitive
.ind	.indication service primitive
.req	.request service primitive
.res	.response service primitive
AA	Application Association
AAA	Authentication Authorization and Accounting
ACK	Acknowledgement
AARE	A-Associate Response – an APDU of the ACSE
AARQ	A-Associate Request – an APDU of the ACSE
ABP	Activation by Personalisation
ACPM	Association Control Protocol Machine
ACSE	Association Control Service Element
AE	Application Entity
AES	Advanced Encryption Standard
AL	Application Layer
AP	Application Process
APDU	Application Layer Protocol Data Unit
API	Application Programming Interface
ASE	Application Service Element
ASO	Application Service Object
ATM	Asynchronous Transfer Mode
A-XDR	Adapted Extended Data Representation
base_name	The short_name corresponding to the first attribute (“logical_name”) of a COSEM object
BD	Block Data
BER	Basic Encoding Rules
BFE	Broadcast Frame Exchange
BN	Block Number
BNA	Block Number Acknowledged
BS	Bit string
BTS	Block Transfer Streaming
BTW	Block Transfer Window
CA	Certification Authority
CCA	Clear Channel Assessment
C/D	Compression and Decompression
CF	Control Function
CL	Connectionless
class_id	COSEM interface class identification code
CMP	Certificate Management Protocol. Refer to RFC 4210.
CO	Connection-oriented
CoAP	Constrained Application Protocol (as defined by RFC 7252)
CoAP BT	Constrained Application Protocol Block Transfer (as defined by RFC 7959)

Abbreviation	Meaning
CON	Confirmable
COSEM	Comprehensive Semantic Model for Energy Management
COSEM_on_IP	The TCP-UDP/IP based COSEM communication profile
CRC	Cyclic Redundancy Check
CRL	Certificate revocation list. Refer to **Error! Reference source not found.**.
CSAP	Client Service Access Point
CSMA-CA	Carrier Sense Multiple Access – Channel Access
CSR	Certificate Signing Request
DAG	Directed Acyclic Graph
DCE	Data Communication Equipment (communications interface or modem)
DCS	Data Collection System
DevAddr	A 32-bit non-unique identifier assigned to an end-device statically or dynamically after a Join Procedure (depending on the activation mode) (LPWAN)
DEVEUI	An IEEE EUI-64 used to identify the device during the Join Procedure
DFE	Directed Frame Exchange
DFE ULAD	Directed Frame Exchange Upper Layer Application Data
DIO	DODAG Information Object
DISC	Disconnect (a HDLC frame type)
DLMS	Device Language Message Specification
DM	Disconnected Mode (a HDLC frame type)
DODAG	Destination Oriented Directed Acyclic Graph See [RFC 6550].
DSA	Digital Signature Algorithm specified in FIPS PUB 186-4:2013
DSAP	Data Link Service Access Point
DSO	Energy Distribution System Operator
DTE	Data Terminal Equipment (computers, terminals or printers)
EAPOL	Extensible Authentication Protocol Over LAN
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman key agreement protocol
ECDSA	Elliptic Curve Digital Signature Algorithm specified in ANSI X9.62 and FIPS PUB 186-4:2013
ECP	Elliptic Curve Point
EDFE	Exended Directed Frame Exchange
ETX	Expected Transmission Count. Number of expected packet transmissions required for error free reception at destination.
EUI-64	64-bit Extended Unique Identifier
FAN	Field Area Network
FCS	Frame Check Sequence
FD	Fan Data [Link]
FDDI	Fibre Distributed Data Interface
FE	Field Element (in relation with public key algorithms)
FIPS	Federal Information Processing Standard
F/R	Fragmentation and Reassembly
FRMR	Frame Reject (a HDLC frame type)

Abbreviation	Meaning
FTP	File Transfer Protocol
Gr	A GBT APDU received
GAK	Global Authentication Key
GBEK	Global Broadcast Encryption Key
GBT	General Block Transfer
GCM	Galois/Counter Mode (GCM), an algorithm for authenticated encryption with associated data
GCP	Generic Companion Profile
GMAC	A specialization of GCM for generating a message authentication code (MAC) on data that is not encrypted
GMT	Greenwich Mean Time
Gr.X	A field of a GBT APDU received
Gs	A GBT APDU sent
Gs.X	A field of a GBT APDU sent
GSM	Global System for Mobile communications
GUA	Global Unicast Address
GUEK	Global Unicast Encryption Key
GW	Gateway
HCS	Header Check Sequence
HDLC	High-level Data Link Control
HES	Head End System, also known as Data Collection System NOTE The HES may be owned by the energy provider or the utility
HHU	Hand Held Unit
HLS	High Level Security (COSEM)
HMAC	Keyed-Hash Message Authentication Code specified in FIPS 198-1
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
I	Information (a HDLC frame type)
IANA	Internet Assigned Numbers Authority
IC	Interface Class
ICMP	Internet Control Message Protocol
IDevID	Initial Device Identifier. See [FANSPEC]
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
IV	Initialization Vector
KEK	Key Encrypting Key
LAN	Local Area Network
LB	Last Block
LDN	Logical Device Name
LLC	Logical Link Control (Sublayer)
LLS	Low Level Security
LNAP	Local Network Access Point

Abbreviation	Meaning
LPDU	LLC Protocol Data Unit
L-SAP	LLC sublayer Service Access Point
LSB	Least Significant Bit
LSDU	LLC Service Data Unit
m	mandatory, used in conjunction with attribute and method definitions
MAC	Medium Access Control (sublayer)
MAC	Message Authentication Code (cryptography)
MHDS	Multi Hop Delivery Service
MIB	Management Information Base
MPL	Multicast Protocol for Low-Power and Lossy Networks
MSAP	MAC sublayer Service Access Point (in the HDLC based profile, it is equal to the HDLC address)
MSB	Most Significant Bit
MSC	Message Sequence Chart
MSDU	MAC Service Data Unit
MTU	Maximum Transmission Unit
N(R)	Receive sequence Number
N(S)	Send sequence Number
NDM	Normal Disconnected Mode
NGW	Network Gateway
NIST	National Institute of Standards and Technology
NNAP	Neighbourhood Network Access Point
NON	Non-confirmable
NRM	Normal Response Mode
o	optional, used in conjunction with attribute and method definitions
OBIS	Object Identification System
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OOB	Out of Band
OS	Octet string
OSI	Open System Interconnection
OTA	Over The Air
P/F	Poll/Final
PAN	Personal area network
PAN-IE	PAN Information Element
PAR	Positive Acknowledgement with Retransmission
PDU	Protocol data unit
PhL	Physical Layer
PIB	PAN Information Base
PHSDU	PH SDU
PKCS	Public Key Cryptography Standard, established by RSA Laboratories
PKI	Public Key Infrastructure
PLC	Power line carrier
PPP	Point-to-Point Protocol

Abbreviation	Meaning
PSDU	Physical layer Service Data Unit
PSTN	Public Switched Telephone Network
RA	Registration Authority
RG	Radio gateway
RLRE	A-Release Response – an APDU of the ACSE
RLRQ	A-Release Request – an APDU of the ACSE
RNG	Random Number Generator
RNR	Receive Not Ready (a HDLC frame type)
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks. See [RFC 6550].
RQ	Receive Queue
RR	Receive Ready (a HDLC frame type)
RSA	Algorithm developed by Rivest, Shamir and Adelman; specified in ANS X9.31 and PKCS #1.
S	A sequence of blocks in the RQ or SQ
SAP	Service Access Point
SCHC	Static Context Header Compression and fragmentation, a generic framework
SDU	Service Data Unit
SHA	Secure Hash Algorithm; specified in FIPS PUB 180-4:2012
SNMP	Simple Network Management Protocol
SNRM	Set Normal Response Mode (a HDLC frame type)
SQ	Send Queue
SSAP	Server Service Access Point
STR	Streaming
SUP	Supplicant. See [IEEE 802.1x]
tbsCertificate	To be signed certificate
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TL	Transport Layer
TLS	Transport Layer Security
TPDU	Transport Layer Protocol Data Unit
TWA	Two Way Alternate
UA	Unnumbered Acknowledge (a HDLC frame type)
UDP	User Datagram Protocol
UI	Unnumbered Information (a HDLC frame type)
ULA	Unique Local (IPv6) Address
UNC	Unbalanced operation Normal response mode Class
URI	Uniform Resource Identifier
USS	Unnumbered Send Status
V(R)	Receive state Variable
V(S)	Send state Variable
VAA	Virtual Application Association
WPDU	Wrapper Protocol Data Unit
xDLMS ASE	Extended DLMS Application Service Element
Wi-Fi	Wireless Fidelity

Abbreviation	Meaning
See also list of abbreviations specific to a cryptographic algorithm in the relevant clauses.	

3.6 Symbols related to the Galois/Counter Mode

Symbol	Meaning
A	Additional Authenticated Data, AAD
AK	Authentication key, a parameter that is part of the AAD
C	Ciphertext
EK	Encryption key, i.e. the block cipher key
IC	Invocation counter, part of the initialization vector. See also invocation field.
IV	Initialization Vector
$len(X)$	The bit length of the bit string X.
$LEN(X)$	The octet length of the octet string X.
P	Plaintext
SC	Security Control Byte
SH	Security Header
$Sys\text{-}T$	System title
T	Authentication tag
t	The bit length of the authentication tag. NOTE This is the same as $\text{len}(T)$
$X \; II \; Y$	Concatenation of two strings, X and Y.

3.7 Symbols related the ECDSA algorithm

Symbol	Meaning
d	The ECDSA private key, which is an integer in the interval $[1, n-1]$.
$Q = (x_Q, y_Q)$	An ECDSA public key. The coordinates x_Q and y_Q are integers in the interval $[0, q-1]$, and $Q = dG$.
k	The ECDSA per-message secret number, which is an integer in the interval $[1, n-1]$.
r	One component of an ECDSA digital signature. It is an integer in $[1, n-1]$. See the definition of (r, s).
s	One component of an ECDSA digital signature. It is an integer in $[1, n-1]$. See the definition of (r, s).
(r, s)	An ECDSA digital signature, where r and s are the digital signature components.
M	The message that is signed using the digital signature algorithm.
$\text{Hash}(M)$	The result of a hash computation (message digest or hash value) on message M using an approved hash function.

3.8 Symbols related to the key agreement algorithms

Symbol	Meaning
$d_{e,U}$, $d_{e,V}$	Party U's and Party V's ephemeral private keys. These are integers in the range [1, n-1].
$d_{s,U}$, $d_{s,V}$	Party U's and Party V's static private keys. These are integers in the range [1, n-1].
ID_U	The identifier of Party U (the initiator)
ID_V	The identifier of Party V (the responder)
$Q_{e,U}$, $Q_{e,V}$	Party U's and Party V's ephemeral public keys. These are points on the elliptic curve defined by the domain parameters.
$Q_{s,U}$, $Q_{s,V}$	Party U's and Party V's static public keys. These are points on the elliptic curve defined by the domain parameters.
U, V	Represent the two parties in a (pair-wise) key establishment scheme.

Symbol	Meaning
Z	A shared secret (represented as a byte string) that is used to derive secret keying material using a key derivation method. *Source: NIST SP 800-56A Rev. 2: 2013*

3.9 Abbreviations related to the DLMS/COSEM M-Bus communication profile

Abbrev	Term	Standard domain
ACC	Access number field	M-Bus
ALA	Application Layer Address	M-Bus
CFG	Configuration byte	M-Bus
CI_{ELL}	CI field introducing the extended link layer (wireless M-Bus)	M-Bus
CI Field	Control Information field	M-Bus
CI_{TL}	CI field introducing the transport layer	M-Bus
DTSAP	Destination Transport Service Access Point	Telecontrol
ELL	Extended Link Layer	M-Bus
ELLA	Extended Link Layer Address	M-Bus
FIN (bit)	Final Bit	Telecontrol
FT1.2	Data Integrity Format class FT1.2	Telecontrol
FT3	Data Integrity Format Class FT3	Telecontrol
LLA	Link Layer Address	M-Bus
STS	Status byte	M-Bus
STSAP	Source Transport Service Access Point	Telecontrol
wM-Bus	Wireless M-Bus	M-Bus

4 Information exchange in DLMS/COSEM

4.1 General

This Clause 4 introduces the main concepts of information exchange in DLMS/COSEM.

The objective of DLMS/COSEM is to specify a standard for a business domain oriented interface object model for devices and systems, as well as services to access the objects. Communication profiles to transport the messages through various communication media are also specified.

The term "devices" is an abstraction; consequently “device” may be any type of device for which this abstraction is suitable.

The COSEM object model is specified in DLMS UA 1000-1 – Part 2, the “Blue Book”. The COSEM objects provide a view of the functionality of devices through their communication interfaces.

This Technical report, the “Green Book” specifies the DLMS/COSEM application layer, lower protocol layers and communication profiles.

The key characteristics of data exchange using DLMS/COSEM are the following:

- devices can be accessed by various parties: clients and third parties;
- mechanisms to control access to the resources of the device are provided; these mechanisms are made available by the DLMS/COSEM AL and the COSEM objects (“Association SN / LN” object, “Security setup” object);
- security and privacy is ensured by applying cryptographical protection to xDLMS messages and to COSEM data;
- low overhead and efficiency is ensured by various mechanisms including selective access, compact encoding and compression;
- at a site, there may be single or multiple devices. In the case of multiple devices at a site, a single access point can be made available;
- data exchange may take place either remotely or locally. Depending on the capabilities of the device, local and remote data exchange may be performed simultaneously without interfering with each other;
- various communication media can be used on local networks (LN), neighbourhood networks (NN) and wide area networks (WAN).

The key element to ensure that the above requirements are met is the Application Association (AA) – determining the contexts of the data exchange – provided by the DLMS/COSEM AL. For details, see the relevant clauses below.

4.2 Communication model

DLMS/COSEM uses the concepts of the Open Systems Interconnection (OSI) model to model information exchange between devices and data collection systems.

NOTE Information in this context comprises xDLMS messages and COSEM data.

Concepts, names and terminology used below relate to the OSI reference model described in ISO/IEC 7498-1:1994. Their use is outlined in this clause and further developed in other clauses.

Application functions of devices and data collection systems are modelled by application processes (APs).

Communication between APs is modelled by communication between application entities (AEs). An AE represents the communication functions of an AP. There may be multiple sets of OSI communication functions in an AP, so a single AP may be represented by multiple AEs. However, each AE represents a single AP. An AE contains a set of communication capabilities called application service elements (ASEs). An ASE is a coherent set of integrated functions. These ASEs may be used independently or in combination. See also 9.1.2.

Data exchange between data collection systems and devices is based on the client/server model where data collection systems play the role of the client and devices play the role of the server. The client sends service requests to the server which sends service responses. In addition the server may initiate unsolicited service requests to inform the client about events or to send data on pre-configured conditions. See also 4.6.

In general, the client and the server APs are located in separate devices. Therefore, message exchange takes place via a protocol stack as shown in Figure 2.

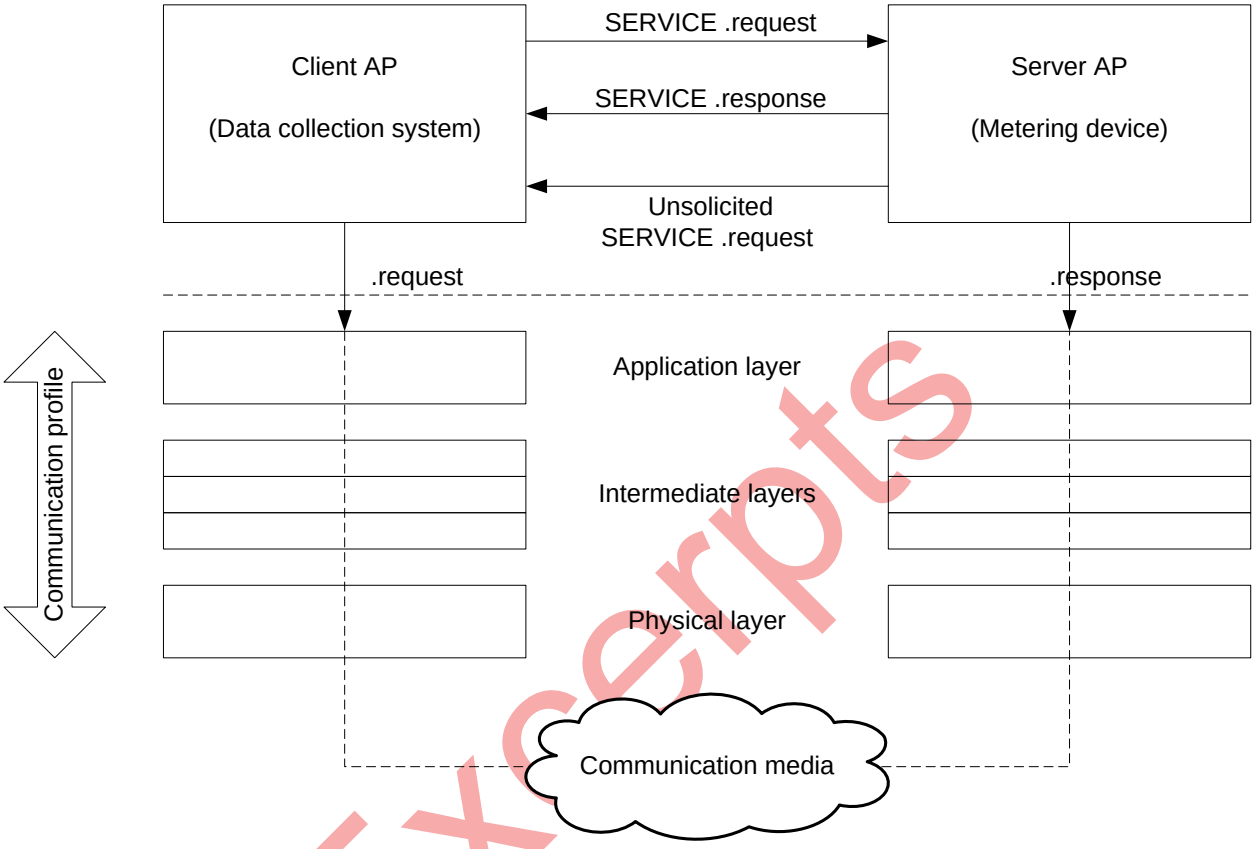

Figure 2 – Client–server model and communication protocols

4.3 Naming and addressing

4.3.1 General

Naming and addressing are important aspects in communication systems. A name identifies a communicating entity. An address identifies where that entity can be found. Names are mapped to addresses; this is known as the process of binding. Figure 3 shows the main elements of naming and addressing in DLMS/COSEM.

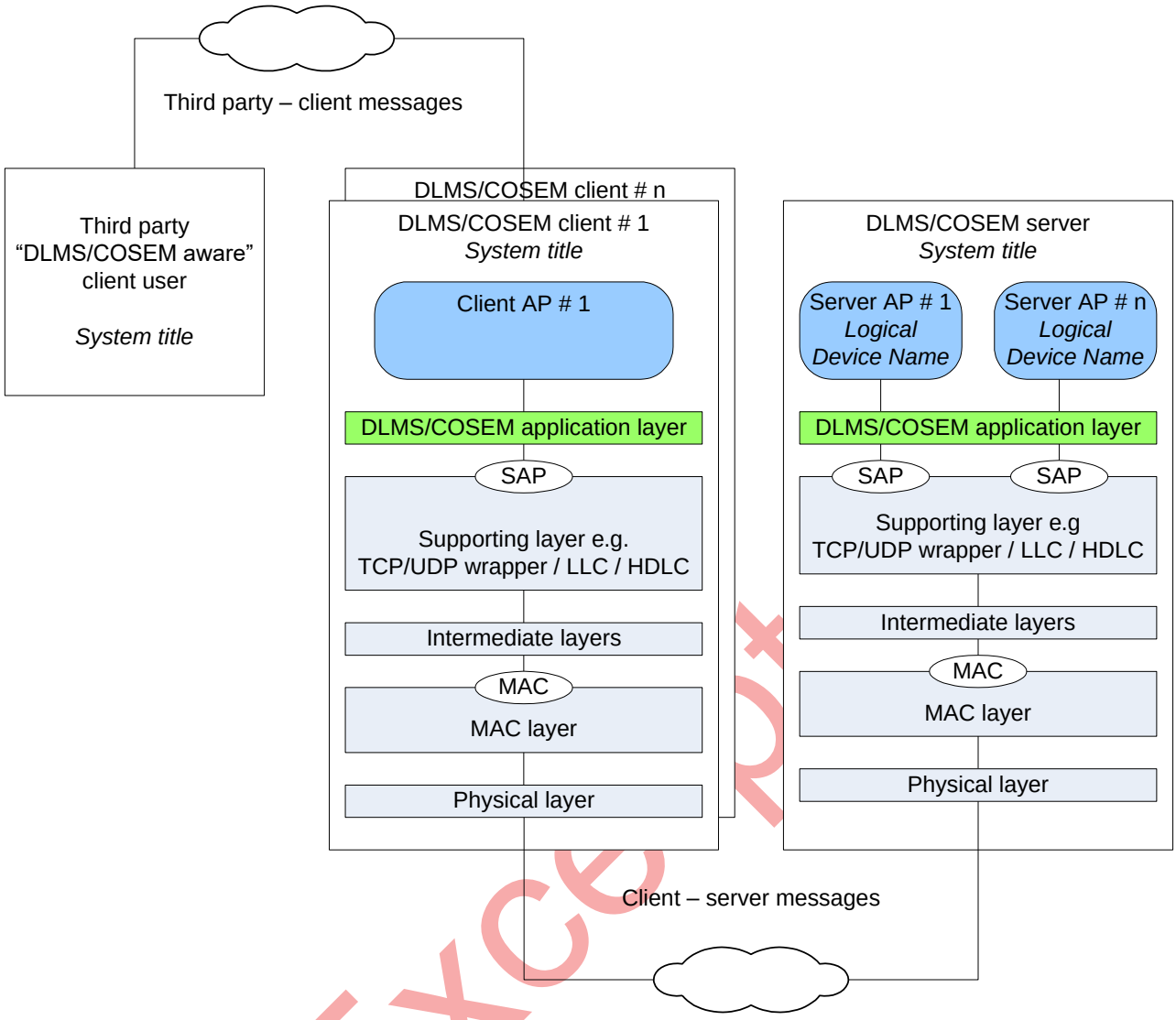

Figure 3 – Naming and addressing in DLMS/COSEM

4.3.2 Naming

DLMS/COSEM entities, including clients, servers as well as third party systems shall be uniquely named by their *system title*. System titles shall be permanently assigned.

Server physical devices may host one or more logical devices (LDs). LDs shall be uniquely identified by their Logical Device Name (LDN). LDs hosted by the same physical device share the system title. System titles are specified in 4.3.4. Logical device names are specified in 4.3.5.

4.3.3 Addressing

Each physical device shall have an appropriate address. It depends on the communication profile and may be a phone number, a MAC address, an IP network address, a CoAP URI, or a combination of these.

NOTE For example, in the case of the 3-layer, connection-oriented, HDLC based communication profile, the lower HDLC address is the MAC address.

Physical device addresses may be pre-configured or may be assigned during a registration process, which also involves binding between the addresses and the system titles.

Each DLMS client and each server – a COSEM logical device – is bound to a Service Access Point (SAP). The SAPs reside in the supporting layer of the DLMS/COSEM AL. Depending on the communication profile the SAP may be a TCP-UDP/IP wrapper address, a CoAP wrapper address, an

upper HDLC address, an LLC address etc. On the server side, this binding is modelled by the “SAP Assignment” IC; see DLMS UA 1000-1 Part 2 Ed.17:2025, 4.4.5.

The values of the SAPs on the client and the server side are specified in Table 1. The length of the SAPs depends on the communication profile.

Table 1 – Client and server SAPs

Client SAPs	
No-station	0x00
Client Management Process / CIASE [1]	0x01
Public Client	0x10
Open for client AP assignment	0x02 …0x0F
	0x11 and up
Server SAPs	
No-station / CIASE [1]	0x00
Management Logical Device	0x01
Reserved for future use	0x02…0x0F
Open for server SAP assignment	0x10 and up
All-station (Broadcast)	Communication profile specific
[1] In the case of the DLMS/COSEM S-FSK PLC profile, see 10.5.	
NOTE Depending on the supporting protocol layer, the SAPs may be represented on one or more bytes.	

4.3.4 System title

The system title *Sys-T* shall uniquely identify each DLMS/COSEM entity. This may be a server, a client or a third party that can access servers via clients. The system title:

- shall be 8 octets long;
- shall be unique.

The first three (most significant) octets should hold the three-letter manufacturer ID[1]. This is the same as the first three octets of the Logical Device Name, see 4.3.5. The remaining 5 octets shall ensure uniqueness.

NOTE The system title can be derived for example from the last 12 digits of the manufacturing number, up to 999 999 999 999. This value converts to 0xE8D4A50FFF. Values above this, up to 0xFFFFFFFFFF (decimal 1 099 511 627 775) can also be used, but these values cannot be mapped to the last 12 digits of the manufacturing number.

Project specific companion specifications may specify a different structure. In that case, the details should be specified by the naming authority designated for the project.

The use of the system title in cryptographic protection of xDLMS messages and COSEM data is further specified in 9.2.3 and 9.2.7.

The client and server require knowledge of each others’ system titles before the cryptographic security algorithms can be used in a ciphered application context. The following options are available for the exchange of system titles:

- during the communication media specific registration process.
  For example, when the S-FSK PLC profile is used, system titles are exchanged during the registration process using the CIASE protocol; see 10.5.5;

[1] Administered by the FLAG Association in co-operation with the DLMS UA.

- in all communication profiles, during AA establishment using the COSEM-OPEN service carried the AARQ / AARE APDU (see 9.3.2). If the system titles sent / received during AA establishment are not the same as the ones exchanged during the registration process, the AA shall be rejected;
- by writing the *client_system_title* attribute and by reading the *server_system_title* attribute of "Security setup" objects, see DLMS UA 1000-1 Part 2 Ed.17:2025, 4.4.7.

In the case of broadcast communication the client can send its system title to all servers, but it has to retrieve the system title of each server one by one.

4.3.5 Logical Device Name

Logical Device Name (LDN) shall be as specified in DLMS UA 1000-1 Part 2 Ed.17:2025, 4.1.8.2.

4.3.6 Client user identification

The client user identification mechanism allows a server to distinguish between different users on the client side and to log their activities accessing the device. It is specified in DLMS UA 1000-1 Part 2 Ed.17:2025, 4.4.2. Naming of client users is outside the scope of this Technical Report.

4.4 Connection oriented operation

The DLMS/COSEM AL is connection oriented. See also 9.1.3.

A communication session consists of three phases, as it is shown in Figure 4:

- first, an application level connection, called Application Association (AA), is established between a client and a server AE; see also 9.1.3. Before initiating the establishment of an AA, the peer PhLs of the client and server side protocol stacks have to be connected. The intermediate layers may have to be connected or not. Each layer, which needs to be connected, may support one or more connections simultaneously;
- once the AA is established, message exchange can take place;
- at the end of the data exchange, the AA is released.

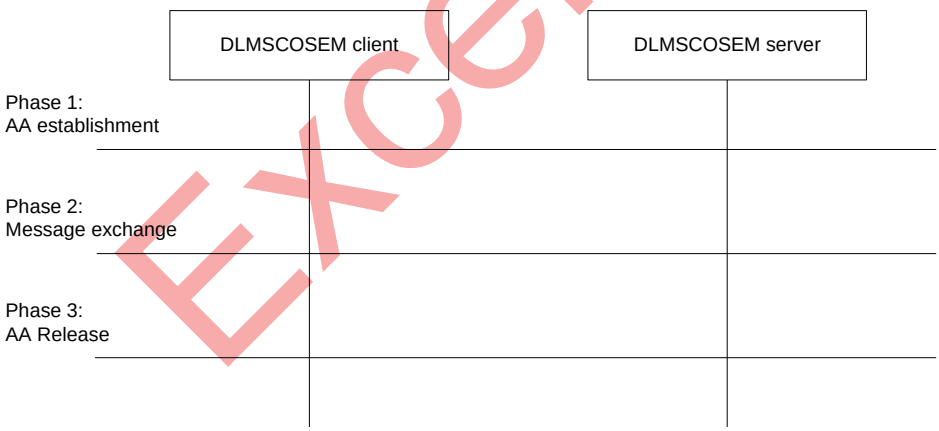

Figure 4 – A complete communication session in the CO environment

For the purposes of very simple devices, one-way communicating devices, and for multicasting and broadcasting pre-established AAs are also allowed. For such AAs the full communication session may include only the message exchange phase: it can be considered that the connection establishment phase has been already done somewhere in the past. Pre-established AAs cannot be released. See also 9.4.4.4.