



BSI Standards Publication

Electricity metering data exchange — The DLMS®/COSEM suite

Part 5-3: DLMS®/COSEM application layer

National foreword

This British Standard is the UK implementation of EN IEC 62056-5-3:2023. It is identical to IEC 62056-5-3:2023. It supersedes BS EN 62056-5-3:2017, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/13, Electricity Meters.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 16070 3

ICS 17.220; 17.220.20; 29.080.30; 35.110; 91.140.50

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2023.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Electricity metering data exchange - The DLMS®/COSEM suite -
Part 5-3: DLMS®/COSEM application layer
(IEC 62056-5-3:2023)

Échange des données de comptage de l'électricité - La
suite DLMS®/COSEM - Partie 5-3: Couche application
DLMS®/COSEM
(IEC 62056-5-3:2023)

Datenkommunikation der elektrischen Energiemessung -
DLMS®/COSEM - Teil 5-3: DLMS®/COSEM-
Anwendungsschicht
(IEC 62056-5-3:2023)

This European Standard was approved by CENELEC on 2023-11-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 13/1890/FDIS, future edition 4 of IEC 62056-5-3, prepared by IEC/TC 13 "Electrical energy measurement and control" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62056-5-3:2023.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2024-08-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2026-11-02

This document supersedes EN 62056-5-3:2017 and all of its amendments and corrigenda (if any).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a Standardization Request addressed to CENELEC by the European Commission.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 62056-5-3:2023 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

ISO 3166 (series) NOTE Approved as EN ISO 3166 (series)

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	EN 61334-4-41	1996
IEC 61334-6	2000	Distribution automation using distribution line carrier systems - Part 6: A-XDR encoding rule	EN 61334-6	2000
IEC/TR 62051	1999	Electricity metering - Glossary of terms	-	-
IEC/TR 62051-1	2004	Electricity metering - Data exchange for meter reading, tariff and load control - Glossary of terms - Part 1: Terms related to data exchange with metering equipment using DLMS®/COSEM	-	-
IEC 62056-6-2	2023	Electricity metering data exchange - The DLMS®/COSEM suite - Part 6-2: COSEM interface classes	EN IEC 62056-6-2	2023
IEC 62056-7-3	2017	Electricity metering data exchange - The DLMS®/COSEM suite - Part 7-3: Wired and wireless M-Bus communication profiles for local and neighbourhood networks	EN 62056-7-3	2017
IEC 62056-7-6	2013	Electricity metering data exchange - The DLMS®/COSEM suite - Part 7-6: The 3-layer, connection-oriented HDLC based communication profile	EN 62056-7-6	2013
IEC 62056-8-3	2013	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-3: Communication profile for PLC S-FSK neighbourhood networks	EN 62056-8-3	2013

EN IEC 62056-5-3:2023 (E)

IEC 62056-8-11	— ¹	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-11: Communication profile for Wi-SUN field area mesh networks	EN IEC 62056-8-11	— ²
IEC 62056-8-12	2023	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-12: Communication profile for Low-Power Wide Area Networks (LPWANs)	EN IEC 62056-8-12	2023
IEC 62056-9-7	2013	Electricity metering data exchange - The DLMS/COSEM suite - Part 9-7: Communication profile for TCP-UDP/IP networks	EN 62056-9-7	2013
ISO/IEC 8824-1	2008	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	-	-
ISO/IEC 8825-1	2008	Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	-	-
ISO/IEC 15953	1999	Information technology - Open systems interconnection - Service definition for the Application service object association control service element	-	-
ISO/IEC 15954	1999	Information technology - Open systems interconnection - Connection-mode protocol for the application service object association control service element	-	-
ISO/IEC 7498-1	1994	Information technology - Open Systems Interconnection - Basic reference model: The basic model	-	-
ITU-T X.509	2008	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-
ITU-T X.693	2008	Information technology - ASN.1 encoding rules: XML Encoding rules (XER)	-	-
ITU-T X.693 Corrigendum 1	2011	Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1	-	-
ITU-T X.694	2008	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1	-	-
ITU-T X.694 Corrigendum	2011	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical corrigendum 1	-	-
FIPS PUB 180-4	2012	Secure Hash Standard (SHS)	-	-
FIPS PUB 186-4	2013	Digital Signature Standard (DSS)	-	-

¹ Under preparation. Stage at the time of publication: IEC CDV.

² Under preparation. Stage at the time of publication: prEN IEC 62056-8-11:2023.

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 800-56A rev2	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)	-	-
NSA2	-	Suite B Implementer's guide to NIST SP800-56A, 28 th July 2009	-	-
NSA3	-	NSA Suite B Base Certificate and CRL Profile, 27 th May 2008	-	-
SEC1	2009	Standards for Efficient Cryptography: Elliptic Curve Cryptography. SECG. Version 2.0	-	-
RFC 3394	2002	Internet Engineering Task Force (IETF). Advanced Encryption Standard (AES) Key Wrap Algorithm. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories)	-	-
RFC 4106	-	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	-	-
RFC 4108	2005	Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages	-	-
RFC 5280	2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-

CONTENTS

FOREWORD.....	12
INTRODUCTION.....	14
1 Scope.....	15
2 Normative references	15
3 Terms, definitions, abbreviated terms and symbols.....	17
3.1 General DLMS®/COSEM definitions	17
3.2 Definitions related to cryptographic security	22
3.3 Definitions and abbreviated terms related to the Galois/Counter Mode.....	32
3.4 General abbreviated terms.....	34
3.5 Symbols related to the Galois/Counter Mode	38
3.6 Symbols related the ECDSA algorithm	38
3.7 Symbols related to the key agreement algorithms	39
4 Overview of DLMS®/COSEM	39
4.1 Information exchange in DLMS®/COSEM	39
4.1.1 General	39
4.1.2 Communication model	40
4.1.3 Naming and addressing	41
4.1.4 Connection oriented operation.....	44
4.1.5 Application associations	45
4.1.6 Messaging patterns	46
4.1.7 Data exchange between third parties and DLMS®/COSEM servers	47
4.1.8 Communication profiles	48
4.1.9 Model of a DLMS®/COSEM metering system.....	50
4.1.10 Model of DLMS®/COSEM servers.....	50
4.1.11 Model of a DLMS®/COSEM client.....	52
4.1.12 Interoperability and interconnectivity in DLMS®/COSEM	53
4.1.13 Ensuring interconnectivity: the protocol identification service.....	53
4.1.14 System integration and meter installation	53
4.2 DLMS®/COSEM application layer main features	54
4.2.1 General	54
4.2.2 DLMS®/COSEM application layer structure	54
4.2.3 The Association Control Service Element, ACSE	55
4.2.4 The xDLMS application service element	56
4.2.5 Layer management services	64
4.2.6 Summary of DLMS®/COSEM application layer services.....	64
4.2.7 DLMS®/COSEM application layer protocols.....	65
5 Information security in DLMS®/COSEM.....	65
5.1 Overview.....	65
5.2 The DLMS®/COSEM security concept	65
5.2.1 Overview	65
5.2.2 Identification and authentication	66
5.2.3 Security context.....	69
5.2.4 Access rights	69
5.2.5 Application layer message security	69
5.2.6 COSEM data security	72
5.3 Cryptographic algorithms	72

5.3.1	Overview	72
5.3.2	Hash function	72
5.3.3	Symmetric key algorithms	73
5.3.4	Public key algorithms	80
5.3.5	Random number generation	90
5.3.6	Compression	91
5.3.7	Security suite	91
5.4	Cryptographic keys – overview	92
5.5	Key used with symmetric key algorithms	92
5.5.1	Symmetric keys types	92
5.5.2	Key information with general-ciphering APDU and data protection	94
5.5.3	Key identification	94
5.5.4	Key wrapping	95
5.5.5	Key agreement	95
5.5.6	Symmetric key cryptoperiods	96
5.6	Keys used with public key algorithms	96
5.6.1	Overview	96
5.6.2	Key pair generation	96
5.6.3	Public key certificates and infrastructure	97
5.6.4	Certificate and certificate extension profile	100
5.6.5	Suite B end entity certificate types to be supported by DLMS®/COSEM servers	108
5.6.6	Management of certificates	108
5.7	Applying cryptographic protection	113
5.7.1	Overview	113
5.7.2	Protecting xDLMS APDUs	113
5.7.3	Multi-layer protection by multiple parties	126
5.7.4	HLS authentication mechanisms	127
5.7.5	Protecting COSEM data	130
6	DLMS®/COSEM application layer service specification	131
6.1	Service primitives and parameters	131
6.2	The COSEM-OPEN service	133
6.3	The COSEM-RELEASE service	138
6.4	COSEM-ABORT service	141
6.5	Protection and general block transfer parameters	141
6.6	The GET service	146
6.7	The SET service	149
6.8	The ACTION service	153
6.9	The ACCESS service	156
6.9.1	Overview – Main features	156
6.9.2	Service specification	158
6.10	The DataNotification service	162
6.11	The EventNotification service	164
6.12	The TriggerEventNotificationSending service	165
6.13	Variable access specification	166
6.14	The Read service	166
6.15	The Write service	170
6.16	The UnconfirmedWrite service	173
6.17	The InformationReport service	173

6.18	Client side layer management services: the SetMapperTable.request	176
6.19	Summary of services and LN/SN data transfer service mapping	176
7	DLMS®/COSEM application layer protocol specification	177
7.1	The control function	177
7.1.1	State definitions of the client side control function	177
7.1.2	State definitions of the server side control function	179
7.2	The ACSE services and APDUs	181
7.2.1	ACSE functional units, services and service parameters	181
7.2.2	Registered COSEM names	184
7.2.3	APDU encoding rules	187
7.2.4	Protocol for application association establishment	187
7.2.5	Protocol for application association release	193
7.3	Protocol for the data transfer services	196
7.3.1	Negotiation of services and options – the conformance block	196
7.3.2	Confirmed and unconfirmed service invocations	197
7.3.3	Protocol for the GET service	199
7.3.4	Protocol for the SET service	202
7.3.5	Protocol for the ACTION service	205
7.3.6	Protocol for the ACCESS service	207
7.3.7	Protocol of the DataNotification service	208
7.3.8	Protocol for the EventNotification service	211
7.3.9	Protocol for the Read service	212
7.3.10	Protocol for the Write service	215
7.3.11	Protocol for the UnconfirmedWrite service	219
7.3.12	Protocol for the InformationReport service	220
7.3.13	Protocol of general block transfer mechanism	221
7.3.14	Protocol of exception mechanism	243
8	Abstract syntax of ACSE and COSEM APDUs	244
9	COSEM APDU XML schema	263
9.1	General	263
9.2	XML Schema	263
Annex A (normative) Using the DLMS®/COSEM application layer in various communications profiles		285
A.1	General	285
A.2	Targeted communication environments	285
A.3	The structure of the profile	285
A.4	Identification and addressing schemes	285
A.5	Supporting layer services and service mapping	286
A.6	Communication profile specific parameters of the COSEM AL services	286
A.7	Specific considerations / constraints using certain services within a given profile	286
A.8	The 3-layer, connection-oriented, HDLC based communication profile	286
A.9	The TCP-UDP/IP based communication profiles (COSEM_on_IP)	286
A.10	The wired and wireless M-Bus communication profiles	286
A.11	The S-FSK PLC profile	286
Annex B (normative) SMS short wrapper		287
Annex C (normative) Gateway protocol		288
C.1	General	288
C.2	The gateway protocol	289

C.3	HES in the WAN/NN acting as Initiator (Pull operation)	290
C.4	End devices in the LAN acting as Initiators (Push operation).....	291
C.4.1	General	291
C.4.2	End device with WAN/NN knowledge	291
C.4.3	End devices without WAN/NN knowledge	291
C.5	Security	291
Annex D (informative)	AARQ and AARE encoding examples	292
D.1	General.....	292
D.2	Encoding of the xDLMS InitiateRequest / InitiateResponse APDU	292
D.3	Specification of the AARQ and AARE APDUs	295
D.4	Data for the examples	296
D.5	Encoding of the AARQ APDU	297
D.6	Encoding of the AARE APDU	300
Annex E (informative)	Encoding examples: AARQ and AARE APDUs using a ciphered application context	306
E.1	A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key.....	306
E.2	Authenticated encryption of the xDLMS InitiateRequest APDU	307
E.3	The AARQ APDU	308
E.4	A-XDR encoding of the xDLMS InitiateResponse APDU	310
E.5	Authenticated encryption of the xDLMS InitiateResponse APDU	311
E.6	The AARE APDU	312
E.7	The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU)	314
E.8	The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU)	315
Annex F (informative)	Data transfer service examples	316
F.1	GET / Read, SET / Write examples	316
F.2	ACCESS service example	333
F.3	Compact array encoding example	334
F.3.1	General	334
F.3.2	The specification of compact-array	335
F.3.3	Example 1: Compact array encoding an array of five long-unsigned values.....	336
F.3.4	Example 2: Compact-array encoding of five octet-string values	337
F.3.5	Example 3: Encoding of the buffer of a Profile generic object	338
F.4	Profile generic IC buffer attribute encoding examples	339
F.4.1	General	339
F.4.2	Get-response with Profile generic normal encoding example	340
F.4.3	Get-response with Profile generic null-data compressed encoding example.....	342
F.4.4	Get-response with Profile generic compact-array encoding example	345
F.4.5	Get-response with Profile generic null-data and delta-value encoding example.....	347
F.4.6	Comparison of various encoding methods for Get-response APDU	350
F.4.7	Combination of the various encoding methods and V.44 compression	350
Annex G (normative)	NSA Suite B elliptic curves and domain parameters	352
Annex H (informative)	Example of an End entity signature certificate using P-256 signed with P-256	354
H.1	Fields of public key certificates	354
H.2	Example of a Root-CA Certificate using P-256 signed with P-256	355

H.3	Example of an end entity digital signature Certificate using P-256 signed with P-256	356
Annex I (normative)	Use of key agreement schemes in DLMS®/COSEM.....	357
I.1	Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	357
I.2	One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme	360
I.3	Static Unified Model C(0e, 2s, ECC CDH) scheme	363
Annex J (informative)	Exchanging protected xDLMS APDUs between TP and server	367
J.1	General.....	367
J.2	Example 1: Protection is the same in the two directions	367
J.3	Example 2: Protection is different in the two directions	368
Annex K (informative)	Significant technical changes with respect to IEC 62056-5-3:2017	370
Bibliography		373
Figure 1	– Client–server model and communication protocols	41
Figure 2	– Naming and addressing in DLMS®/COSEM	42
Figure 3	– A complete communication session in the CO environment	44
Figure 4	– DLMS®/COSEM messaging patterns	47
Figure 5	– DLMS®/COSEM generic communication profile	49
Figure 6	– Model of a DLMS®/COSEM metering system	50
Figure 7	– DLMS®/COSEM server model.....	51
Figure 8	– Model of a DLMS®/COSEM client using multiple protocol stacks.....	52
Figure 9	– The structure of the DLMS®/COSEM application layers	54
Figure 10	– The concept of composable xDLMS messages.....	61
Figure 11	– Summary of DLMS®/COSEM AL services	64
Figure 12	– Authentication mechanisms.....	67
Figure 13	– Client – server message security concept	70
Figure 14	– End-to-end message security concept.....	71
Figure 15	– Hash function	73
Figure 16	– Encryption and decryption	74
Figure 17	– Message Authentication Codes (MACs).....	75
Figure 18	– GCM functions	77
Figure 19	– Digital signatures	83
Figure 20	– C(2e, 0s) scheme: each party contributes only an ephemeral key pair.....	85
Figure 21	– C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair	86
Figure 22	– C(0e, 2s) scheme: each party contributes only a static key pair.....	88
Figure 23	– Architecture of a Public Key Infrastructure (example)	99
Figure 24	– MSC for provisioning the server with CA certificates	109
Figure 25	– MSC for security personalisation of the server	110
Figure 26	– Provisioning the server with the certificate of the client	111
Figure 27	– Provisioning the client / third party with a certificate of the server.....	112
Figure 28	– Remove certificate from the server.....	112
Figure 29	– Cryptographic protection of information using AES-GCM.....	116
Figure 30	– Structure of service-specific global / dedicated ciphering xDLMS APDU.....	118

Figure 31 – Structure of general-glo-ciphering and general-ded-ciphering xDLMS APDUs	119
Figure 32 – Structure of general-ciphering xDLMS APDUs	120
Figure 33 – Structure of general-signing APDUs	126
Figure 34 – Service primitives	131
Figure 35 – Time sequence diagrams	132
Figure 36 – Additional service parameters to control cryptographic protection and GBT	142
Figure 37 – Partial state machine for the client side control function	178
Figure 38 – Partial state machine for the server side control function	180
Figure 39 – MSC for successful AA establishment preceded by a successful lower layer connection establishment	189
Figure 40 – Graceful AA release using the A-RELEASE service	194
Figure 41 – Graceful AA release by disconnecting the supporting layer	195
Figure 42 – Aborting an AA following a PH-ABORT.indication	196
Figure 43 – MSC of the GET service	199
Figure 44 – MSC of the GET service with block transfer	200
Figure 45 – MSC of the GET service with block transfer, long GET aborted	202
Figure 46 – MSC of the SET service	203
Figure 47 – MSC of the SET service with block transfer	203
Figure 48 – MSC of the ACTION service	205
Figure 49 – MSC of the ACTION service with block transfer	207
Figure 50 – Access Service with long response	208
Figure 51 – Access Service with long request and response	208
Figure 52 – MSC for the DataNotification service, case 1)	209
Figure 53 – MSC for the DataNotification service, case 2)	210
Figure 54 – MSC for the DataNotification service, case 3)	211
Figure 55 – MSC of the Read service used for reading an attribute	214
Figure 56 – MSC of the Read service used for invoking a method	214
Figure 57 – MSC of the Read Service used for reading an attribute, with block transfer	215
Figure 58 – MSC of the Write service used for writing an attribute	218
Figure 59 – MSC of the Write service used for invoking a method	218
Figure 60 – MSC of the Write Service used for writing an attribute, with block transfer	219
Figure 61 – MSC of the Unconfirmed Write service used for writing an attribute	220
Figure 62 – Partial service invocations and GBT APDUs	223
Figure 63 – The GBT procedure	226
Figure 64 – Send GBT APDU stream sub-procedure	230
Figure 65 – Process GBT APDU sub-procedure	232
Figure 66 – Check RQ and fill gaps sub-procedure	234
Figure 67 – GET service with GBT, switching to streaming	235
Figure 68 – GET service with partial invocations, GBT and streaming, recovery of 4 th block sent in the 2 nd stream	236
Figure 69 – GET service with partial invocations, GBT and streaming, recovery of 4 th and 5 th block	238

Figure 70 – GET service with partial invocations, GBT and streaming, recovery of last block.....	239
Figure 71 – SET service with GBT, with server not supporting streaming, recovery of 3 rd block.....	240
Figure 72 – ACTION-WITH-LIST service with bi-directional GBT and block recovery	241
Figure 73 – DataNotification service with GBT with partial invocation.....	243
Figure B.1 – Short wrapper	287
Figure C.1 – General architecture with gateway	288
Figure C.2 – The fields used for pre-fixing the COSEM APDUs	289
Figure C.3 – Pull message sequence chart	290
Figure C.4 – Push message sequence chart	291
Figure I.1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	357
Figure I.2 – Ciphered xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme.....	360
Figure I.3 – Ciphered xDLMS APDU protected by an ephemeral key established using the Static Unified Model C(0e, 2s, ECC CDH) scheme	364
Figure J.1 – Exchanging protected xDLMS APDUs between TP and server: example 1.....	368
Figure J.2 – Exchanging protected xDLMS APDUs between TP and server: example 2.....	369
Table 1 – Client and server SAPs	43
Table 2 – Clarification of the meaning of PDU size for DLMS®/COSEM	63
Table 3 – Elliptic curves in DLMS®/COSEM security suites	81
Table 4 – Ephemeral Unified Model key agreement scheme summary	85
Table 5 – One-pass Diffie-Hellman key agreement scheme summary	87
Table 6 – Static Unified Model key agreement scheme summary	89
Table 7 – <i>OtherInfo</i> subfields and substrings	90
Table 8 – Security algorithm ID-s	90
Table 9 – DLMS®/COSEM security suites.....	91
Table 10 – Symmetric keys types.....	93
Table 11 – Key information with general-ciphering APDU and data protection.....	94
Table 12 – Asymmetric keys types and their use.....	96
Table 13 – X.509 v3 Certificate structure	100
Table 14 – X.509 v3 tbsCertificate fields	101
Table 15 – Naming scheme for the Root-CA instance (informative).....	102
Table 16 – Naming scheme for the Sub-CA instance (informative).....	102
Table 17 – Naming scheme for the end entity instance	103
Table 18 – X.509 v3 Certificate extensions	105
Table 19 – Key Usage extensions	106
Table 20 – Subject Alternative Name values	106
Table 21 – Issuer Alternative Name values	107
Table 22 – Basic constraints extension values	107
Table 23 – Certificates handled by DLMS®/COSEM end entities.....	108
Table 24 – Security policy values ("Security setup" version 1)	113

Table 25 – Access rights values ("Association LN" ver 3 "Association SN" ver 4).....	114
Table 26 – Ciphered xDLMS APDUs	115
Table 27 – Security control byte.....	117
Table 28 – Plaintext and Additional Authenticated Data	117
Table 29 – Use of the fields of the ciphering xDLMS APDUs	121
Table 30 – Example: glo-get-request xDLMS APDU	122
Table 31 – ACCESS service with general-ciphering, One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) key agreement scheme.....	124
Table 32 – DLMS®/COSEM HLS authentication mechanisms	128
Table 33 – HLS example using authentication-mechanism 5 with GMAC.....	129
Table 34 – HLS example using authentication-mechanism 7 with ECDSA	130
Table 35 – Codes for AL service parameters.....	133
Table 36 – Service parameters of the COSEM-OPEN service primitives	134
Table 37 – Service parameters of the COSEM-RELEASE service primitives	138
Table 38 – Service parameters of the COSEM-ABORT service primitives	141
Table 39 – Additional service parameters	143
Table 40 – Security parameters	144
Table 41 – APDUs used with security protection types.....	145
Table 42 – Service parameters of the GET service	147
Table 43 – GET service request and response types	148
Table 44 – Service parameters of the SET service	150
Table 45 – SET service request and response types	151
Table 46 – Service parameters of the ACTION service.....	153
Table 47 – ACTION service request and response types.....	154
Table 48 – Service parameters of the ACCESS service	159
Table 49 – Service parameters of the DataNotification service primitives	163
Table 50 – Service parameters of the EventNotification service primitives	164
Table 51 – Service parameters of the TriggerEventNotificationSending.request service primitive.....	165
Table 52 – Variable Access Specification.....	166
Table 53 – Service parameters of the Read service	167
Table 54 – Use of the Variable_Access_Specification variants and the Read.response choices	168
Table 55 – Service parameters of the Write service	171
Table 56 – Use of the Variable_Access_Specification variants and the Write.response choices	172
Table 57 – Service parameters of the UnconfirmedWrite service.....	174
Table 58 – Use of the Variable_Access_Specification variants.....	174
Table 59 – Service parameters of the InformationReport service.....	175
Table 60 – Service parameters of the SetMapperTable.request service primitives	176
Table 61 – Summary of ACSE services.....	176
Table 62 – Summary of xDLMS services	177
Table 63 – Functional Unit APDUs and their fields	182
Table 64 – COSEM application context names	186

Table 65 – COSEM authentication mechanism names	186
Table 66 – Cryptographic algorithm ID-s	187
Table 67 – xDLMS Conformance block	197
Table 68 – GET service types and APDUs	199
Table 69 – SET service types and APDUs	202
Table 70 – ACTION service types and APDUs	205
Table 71 – Mapping between the GET and the Read services	212
Table 72 – Mapping between the ACTION and the Read services	213
Table 73 – Mapping between the SET and the Write services	216
Table 74 – Mapping between the ACTION and the Write service	217
Table 75 – Mapping between the SET and the UnconfirmedWrite services	220
Table 76 – Mapping between the ACTION and the UnconfirmedWrite services	220
Table 77 – Mapping between the EventNotification and InformationReport services	221
Table 78 – GBT procedure state variables	228
Table 79 – xDLMS exception mechanism	244
Table B.1 – Reserved Application Processes	287
Table D.1 – Conformance block	293
Table D.2 – A-XDR encoding of the xDLMS InitiateRequest APDU	294
Table D.3 – A-XDR encoding of the xDLMS InitiateResponse APDU	295
Table D.4 – BER encoding of the AARQ APDU	298
Table D.5 – Complete AARQ APDU	300
Table D.6 – BER encoding of the AARE APDU	301
Table D.7 – The complete AARE APDU	305
Table E.1 – A-XDR encoding of the xDLMS InitiateRequest APDU	307
Table E.2 – Authenticated encryption of the xDLMS InitiateRequest APDU	308
Table E.3 – BER encoding of the AARQ APDU	309
Table E.4 – A-XDR encoding of the xDLMS InitiateResponse APDU	311
Table E.5 – Authenticated encryption of the xDLMS InitiateResponse APDU	312
Table E.6 – BER encoding of the AARE APDU	313
Table E.7 – BER encoding of the RLRQ APDU	314
Table E.8 – BER encoding of the RLRE APDU	315
Table F.1 – The objects used in the examples	316
Table F.2 – Example: Reading the value of a single attribute without block transfer	317
Table F.3 – Example: Reading the value of a list of attributes without block transfer	318
Table F.4 – Example: Reading the value of a single attribute with block transfer	320
Table F.5 – Example: Reading the value of a list of attributes with block transfer	322
Table F.6 – Example: Writing the value of a single attribute without block transfer	325
Table F.7 – Example: Writing the value of a list of attributes without block transfer	326
Table F.8 – Example: Writing the value of a single attribute with block transfer	328
Table F.9 – Example: Writing the value of a list of attributes with block transfer	330
Table F.10 – Example: ACCESS service without block transfer	333
Table F.11 – Profile generic buffer – get-response with normal encoding	340
Table F.12 – Profile generic buffer – get-response with null-data compression	342

Table F.13 – Profile generic buffer – get-response with compact-array encoding	345
Table F.14 – Profile generic buffer – Get-response with null-data and delta-value encoding	348
Table F.15 – Comparison of various encoding methods for get-response APDU	350
Table F.16 – Combination of the various encoding methods and V.44 compression for get-response APDU	351
Table G.1 – ECC_P256_Domain_Parameters	352
Table G.2 – ECC_P384_Domain_Parameters	353
Table H.1 – Fields of public key Certificates using P-256 signed with P-256	354
Table I.1 – Test vector for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	358
Table I.2 – Test vector for key agreement using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme	361
Table I.3 – Test vector for key agreement using the Static-Unified Model (0e, 2s, ECC CDH) scheme	365

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRICITY METERING DATA EXCHANGE –
THE DLMS®/COSEM SUITE –****Part 5-3: DLMS®/COSEM application layer****FOREWORD**

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National 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 IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62056-5-3 has been prepared by IEC technical committee 13: Electrical energy measurement and control. It is an International Standard.

This fourth edition cancels and replaces the third edition published in 2017. This edition constitutes a technical revision.

The significant technical changes with respect to the previous edition are listed in Annex K (Informative).

The text of this International Standard is based on the following documents:

Draft	Report on voting
13/1890/FDIS	13/1904/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all the parts in the IEC 62056 series, published under the general title *Electricity metering data exchange – The DLMS®/COSEM suite*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This fourth edition of IEC 62056-5-3 has been prepared by IEC TC13 WG14 with a significant contribution of the DLMS® User Association, its A-type liaison partner.

This edition is in line with DLMS® UA 1000-2, the "Green Book" Ed. 10:2020 and DLMS® UA 1000-2, the "Green Book" Ed. 10 Amendment 1 2021.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning the stack of protocols on which the present standard IEC 62056-5-3 is based.

The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the IEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions for applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the IEC. Information may be obtained from:

DLMS¹ User Association
www.dlms.com

¹ Device Language Message Specification.

ELECTRICITY METERING DATA EXCHANGE – THE DLMS®/COSEM SUITE –

Part 5-3: DLMS®/COSEM application layer

1 Scope

This part of IEC 62056 specifies the DLMS®/COSEM application layer in terms of structure, services and protocols for DLMS®/COSEM clients and servers, and defines rules to specify the DLMS®/COSEM communication profiles.

It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2:2021 using either logical name (LN) or short name (SN) referencing.

Annex A (normative) defines how to use the COSEM application layer in various communication profiles. It specifies how various communication profiles can be constructed for exchanging data with metering equipment using the COSEM interface model, and what are the necessary elements to specify in each communication profile. The actual, media-specific communication profiles are specified in separate parts of the IEC 62056 series.

Annex B (normative) specifies the SMS short wrapper.

Annex C (normative) specifies the gateway protocol.

Annex D, Annex E and Annex F (informative) include encoding examples for APDUs.

Annex G (normative) provides NSA Suite B elliptic curves and domain parameters.

Annex H (informative) provides an example of an End entity signature certificate using P-256 signed with P-256.

Annex I (normative) specifies the use of key agreement schemes in DLMS®/COSEM.

Annex J (informative) provides examples of exchanging protected xDLMS APDUs between a third party and a server.

Annex K (informative) lists the main technical changes in this fourth edition.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61334-4-41:1996, *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocols – Distribution line message specification*

IEC 61334-6:2000, *Distribution automation using distribution line carrier systems – Part 6: A-XDR encoding rule*

IEC TR 62051:1999, *Electricity metering – Glossary of terms*

IEC TR 62051-1:2004, *Electricity metering – Data exchange for meter reading, tariff and load control – Glossary of terms – Part 1: Terms related to data exchange with metering equipment using DLMS®/COSEM*

IEC 62056-6-2:2021, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 6-2: COSEM interface classes*

IEC 62056-7-3:2017, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 7-3: Wired and wireless M-Bus communication profiles for local and neighbourhood networks*

IEC 62056-7-6:2013, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 7-6: The 3-layer, connection-oriented HDLC based communication profile*

IEC 62056-8-3:2013, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-3: Communication profile for PLC S-FSK neighbourhood networks*

IEC 62056-8-11:–² *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-11: Communication profile for Wi-SUN field area mesh networks*

IEC 62056-8-12:–³ *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-12: Communication profile for Low Power Wide Area Networks (LPWAN)*

IEC 62056-9-7:2013, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 9-7: Communication profile for TCP-UDP/IP networks*

ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1) – Part 1: Specification of basic notation*

ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules – Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

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.

ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

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*

² Under preparation. Stage at the time of publication: IEC CDV.

³ Under preparation. Stage at the time of publication: 13/1877/CDV:2023.

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.1 Technical Corrigendum 1*

FIPS PUB 180-4:2012, *Secure hash standard (SHS)*

FIPS PUB 186-4:2013, *Digital Signature Standard (DSS)*

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 800-56A 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)

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

SEC1:2009, *Standards for Efficient Cryptography: Elliptic Curve Cryptography*. SECG. Version 2.0

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002 <http://tools.ietf.org/html/rfc3394>

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)* <http://www.rfc-editor.org/rfc/rfc4106.txt>

RFC 4108, *Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages*, 2005, <http://www.ietf.org/rfc/rfc4108>

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, 2008, <http://www.ietf.org/rfc/rfc5280>

3 Terms, definitions, abbreviated terms and symbols

For the purposes of this document, the terms and definitions given in IEC TR 62051:1999, IEC TR 62051-1, RFC 4106, and the following apply.

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

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

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

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

Companion Specification for Energy Metering; 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 1 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 1 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 1 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

physical metering equipment, the highest level element used in the COSEM interface model of metering equipment

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

application process running in a metering equipment

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 1 to entry: A meter 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 1 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 1 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 document

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

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

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

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

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**

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**

property that sensitive information is not disclosed to unauthorized entities

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

3.2.13**cryptographic algorithm**

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**

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

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**

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

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

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

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 1 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

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

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**

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**

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**

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**

result of applying a hash function to information

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

3.2.28**initialization vector****IV**

vector used in defining the starting point of a cryptographic process

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

3.2.29**identification**

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

(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

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

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

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

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

Note 1 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

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

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**

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**

(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**

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**

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**

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**

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**

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**

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**

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**

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**

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**

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**

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**

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>**

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**

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")

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

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>

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

Note 1 to entry: In DLMS®/COSEM the dedicated key is a session key.

3.2.63 shared secret

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

3.2.68**static 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 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**

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**

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**

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**

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**

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**

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 abbreviated terms related to the Galois/Counter Mode**3.3.1****Additional Authenticated Data****AAD**

input data to the authenticated encryption function that is authenticated but not encrypted

[SOURCE: NIST SP 800-38D:2007]

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

[SOURCE: NIST SP 800-38D:2007]

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

[SOURCE: NIST SP 800-38D:2007]

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

[SOURCE: NIST SP 800-38D:2007]

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

[SOURCE: NIST SP 800-38D:2007]

3.3.6**ciphertext**

encrypted form of the plaintext

[SOURCE: NIST SP 800-38D:2007]

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

[SOURCE: NIST SP 800-38D:2007]

3.3.8**fresh**

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

[SOURCE: NIST SP 800-38D:2007]

3.3.9**GCM**

Galois/Counter Mode

[SOURCE: NIST SP 800-38D:2007]

3.3.10**initialization Vector****IV**

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

Note 1 to entry: For the purposes of this document, the invocation field is the invocation counter.

[SOURCE: NIST SP 800-38D:2007]

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

[SOURCE: NIST SP 800-38D:2007]

3.3.12**key**

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

[SOURCE: NIST SP 800-38D:2007]

3.3.13

plaintext
P

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

[SOURCE: NIST SP 800-38D:2007]

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: $SH = SC \parallel IC$.

3.4 General abbreviated terms

Abbreviation	Meaning
.cnf	.confirm service primitive
.ind	.indication service primitive
.req	.request service primitive
.res	.response service primitive
AA	Application Association
AARE	A-Associate Response – an APDU of the ACSE
AARQ	A-Associate Request – an APDU of the ACSE
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
BER	Basic Encoding Rules
BD	Block Data
BN	Block Number
BNA	Block Number Acknowledged
BS	Bit string
BTS	Block Transfer Streaming
BTW	Block Transfer Window
CA	Certification Authority
CF	Control Function
CL	Connectionless

Abbreviation	Meaning
class_id	COSEM interface class identification code
CMP	Certificate Management Protocol. Refer to RFC 4210.
CO	Connection-oriented
COSEM	Companion Specification for Energy Metering
COSEM_on_IP	The TCP-UDP/IP based COSEM communication profile
CRC	Cyclic Redundancy Check
CRL	Certificate revocation list. Refer to RFC 5280.
CSR	Certificate Signing Request
DCE	Data Communication Equipment (communications interface or modem)
DCS	Data Collection System
DISC	Disconnect (a HDLC frame type)
DLMS®	Device Language Message Specification
DM	Disconnected Mode (a HDLC frame type)
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)
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
EUI-64	64-bit Extended Unique Identifier
FCS	Frame Check Sequence
FDDI	Fibre Distributed Data Interface
FE	Field Element (in relation with public key algorithms)
FIPS	Federal Information Processing Standard
FRMR	Frame Reject (a HDLC frame type)
FTP	File Transfer Protocol
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
GMAC	A specialization of GCM for generating a message authentication code (MAC) on data that is not encrypted
GMT	Greenwich Mean Time
GSM	Global System for Mobile communications
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)

Abbreviation	Meaning
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
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
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)
MIB	Management Information Base
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
N(R)	Receive sequence Number
N(S)	Send sequence Number
NDM	Normal Disconnected Mode
NIST	National Institute of Standards and Technology
NNAP	Neighbourhood Network Access Point
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

Abbreviation	Meaning
OTA	Over The Air
P/F	Poll/Final
PAR	Positive Acknowledgement with Retransmission
PDU	Protocol data unit
PhL	Physical Layer
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
PSDU	Physical layer Service Data Unit
PSTN	Public Switched Telephone Network
RA	Registration Authority
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)
RR	Receive Ready (a HDLC frame type)
RSA	Algorithm developed by Rivest, Shamir and Adelman; specified in ANS X9.31 and PKCS #1.
SAP	Service Access Point
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)
STR	Streaming
tbsCertificate	To be signed certificate
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TL	Transport Layer
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)
UNC	Unbalanced operation Normal response mode Class
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
See also list of abbreviations specific to a cryptographic algorithm in the relevant clauses.	

3.5 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
$\text{len}(X)$	The bit length of the bit string X .
$\text{LEN}(X)$	The octet length of the octet string X .
P	Plaintext
SC	Security Control Byte
SH	Security Header
$\text{Sys-}T$	System title
T	Authentication tag
t	The bit length of the authentication tag. NOTE This is the same as $\text{len}(T)$
$X \parallel Y$	Concatenation of two strings, X and Y .

3.6 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.

3.7 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.
Z	A shared secret (represented as a byte string) that is used to derive secret keying material using a key derivation method. <i>Source: NIST SP 800-56A Rev. 2: 2013</i>

4 Overview of DLMS®/COSEM

4.1 Information exchange in DLMS®/COSEM

4.1.1 General

This subclause 4.1 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 metering 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 "metering devices" is an abstraction; consequently "metering device" may be any type of device for which this abstraction is suitable.

The COSEM object model is specified in IEC 62056-6-2:2021. The COSEM objects provide a view of the functionality of metering devices through their communication interfaces.

This document specifies the DLMS®/COSEM application layer and the rules for specifying DLMS®/COSEM communication profiles; see Annex A.

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

- metering devices can be accessed by various parties: clients and third parties;
- mechanisms to control access to the resources of the metering 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 metering site, there may be single or multiple metering devices. In the case of multiple metering devices at a metering site, a single access point can be made available;
- data exchange may take place either remotely or locally. Depending on the capabilities of the metering 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.

4.1.2 Communication model

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

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

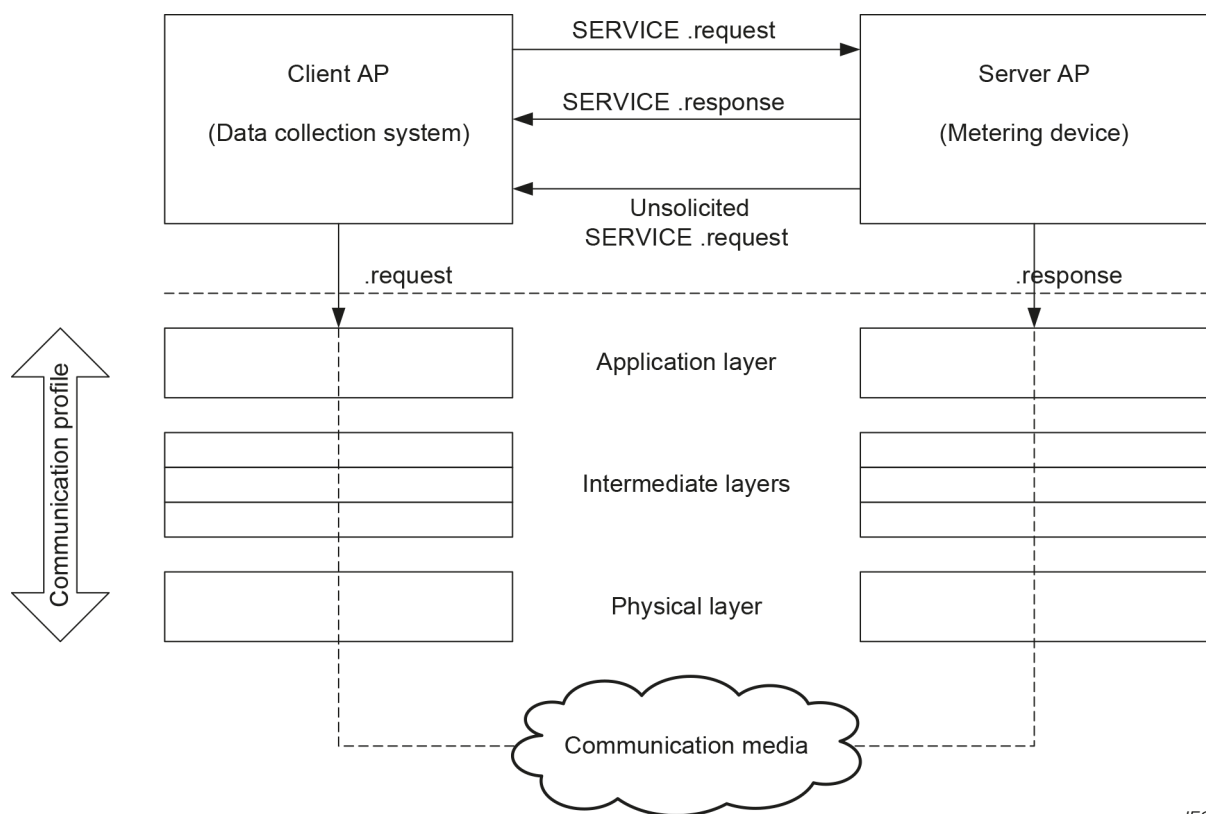
Concepts, names and terminology used below relate to the OSI reference model described in ISO/IEC 7498-1:1994. Their use is outlined in this clause and further developed in other clauses.

Application functions of metering 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 4.2.2.

Data exchange between data collection systems and metering devices is based on the client/server model where data collection systems play the role of the client and metering 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 4.1.6.

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 1.



IEC

Figure 1 – Client-server model and communication protocols

4.1.3 Naming and addressing

4.1.3.1 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 2 shows the main elements of naming and addressing in DLMS®/COSEM.

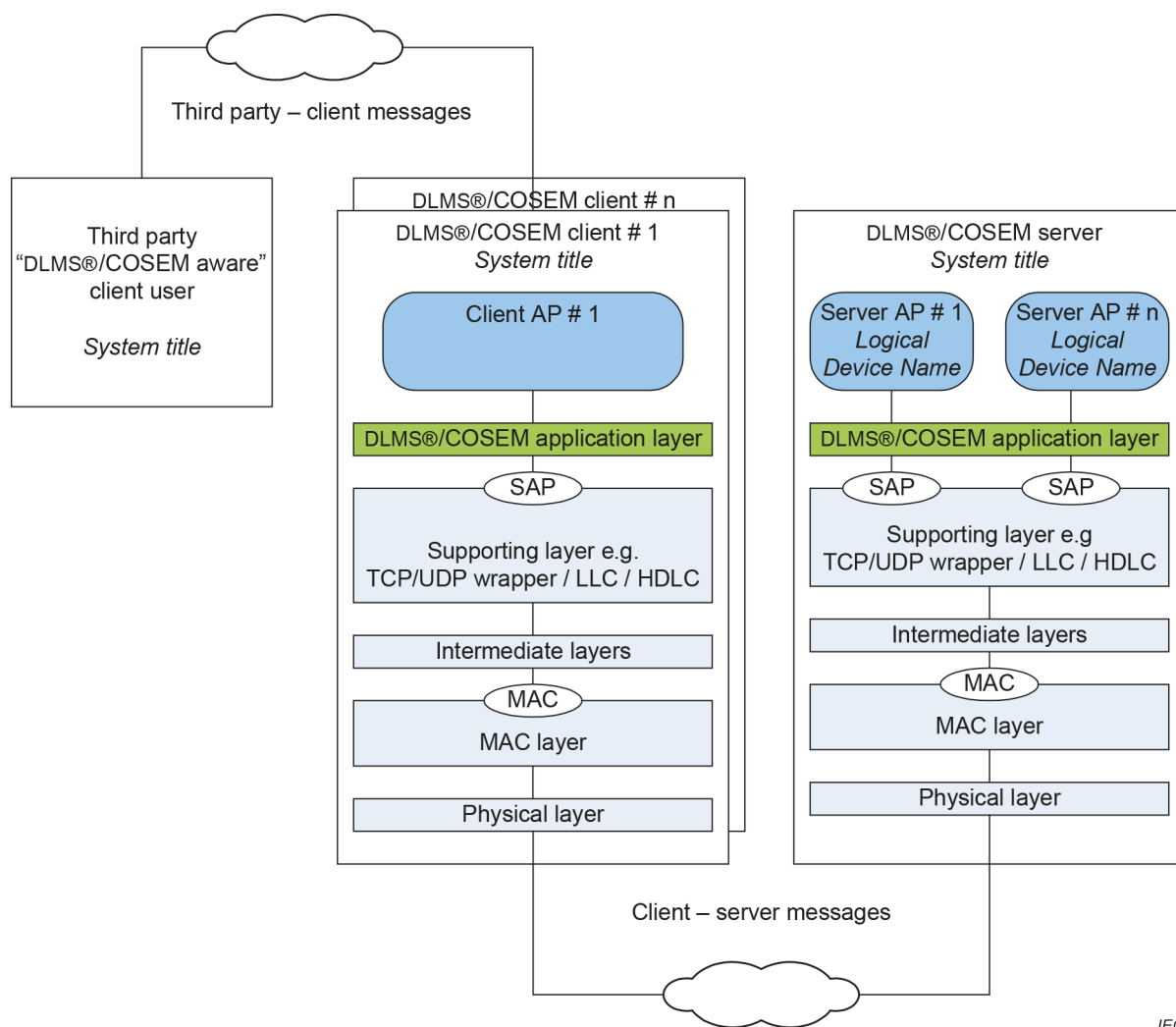


Figure 2 – Naming and addressing in DLMS®/COSEM

4.1.3.2 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 4.1.3.4. Logical device names are specified in 4.1.3.5.

4.1.3.3 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 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®/COSEM 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, an upper HDLC address, an LLC address etc. On the server side, this binding is modelled by the "SAP Assignment" IC; see IEC 62056-6-2:2021, 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 IEC 62056-8-3.	
NOTE Depending on the supporting layer, the SAPs may be represented on one or more bytes.	

4.1.3.4 System title

The system title $Sys-T$ shall uniquely identify each DLMS®/COSEM entity that may be 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 leading (i.e., the 3 leftmost) octets should hold the three-letter manufacturer ID⁴. This is the same as the leading three octets of the Logical Device Name, see 4.1.3.5. The remaining 5 octets shall ensure uniqueness.

NOTE It 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 0xFFFFFFFF (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 as such for the project.

The use of the system title in cryptographic protection of xDLMS messages and COSEM data is further specified in 5.3 and 5.7.

⁴ Administered by the FLAG Association in co-operation with the DLMS UA.

Before the cryptographic security algorithms can be used – this requires a ciphered application context – the peers have to exchange system titles. The following possibilities are available:

- 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 IEC 62056-8-3;
- in all communication profiles, system titles may be exchanged during AA establishment using the COSEM-OPEN service, see 6.2, carried the AARQ / AARE APDU. 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 IEC 62056-6-2:2021, 4.4.7.

In the case of broadcast communication, only the client sends the system title to the server.

4.1.3.5 Logical Device Name

Logical Device Name (LDN) shall be as specified in IEC 62056-6-2:2021, 4.1.4.6.

4.1.3.6 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 meter. It is specified in IEC 62056-6-2:2021, 4.4.2. Naming of client users is outside the scope of this International Standard.

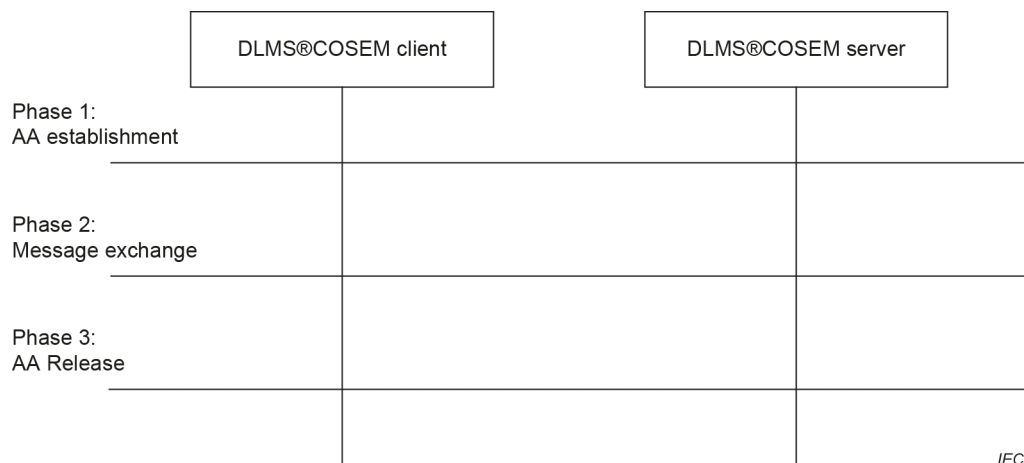
4.1.4 Connection oriented operation

The DLMS®/COSEM AL is connection oriented. See also 4.2.3.

A communication session consists of three phases, as it is shown in Figure 3:

first, an application level connection, called Application Association (AA), is established between a client and a server AE; see also 4.2.3. 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.



IEC

Figure 3 – A complete communication session in the CO environment