

© Copyright SEK Svensk Elstandard. Reproduction in any form without permission is prohibited.

Elmätare – Datakommunikation för avläsning av elmätare och för styrning av tariff och belastning – DLMS/COSEM-familjen – Del 5-3: Tillämpningsskikt DLMS/COSEM

*Electricity metering data exchange –
The DLMS/COSEM suite –
Part 5-3: DLMS/COSEM application layer*

Som svensk standard gäller europastandarden EN IEC 62056-5-3:2023. Den svenska standarden innehåller den officiella engelska språkversionen av EN IEC 62056-5-3:2023.

Nationellt förord

Europastandarden EN IEC 62056-5-3:2023

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 62056-5-3, Fourth edition, 2023 - Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-EN 62056-5-3, utg 3:2018 med eventuella tillägg, ändringar och rättelser gäller ej fr o m 2026-11-02.

ICS 17.220.00; 35.110.00; 91.140.50

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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	-	-

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Electricity metering data exchange – The DLMS®/COSEM suite –
Part 5-3: DLMS®/COSEM application layer**

**Échange des données de comptage de l'électricité – La suite DLMS®/COSEM –
Partie 5-3: Couche application DLMS®/COSEM**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 17.220, 35.110, 91.140.50

ISBN 978-2-8322-7223-7

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

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	175

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 APDUs	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>