IEC 62056-5-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 17.220; 35.110; 91.140.50

ISBN 978-2-8322-4599-6

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 11
INTRODUCTION 13
1 Scope 14
2 Normative references 14
3 Terms, definitions, abbreviated terms and symbols 16
3.1 General DLMS/COSEM definitions 16
3.2 Definitions related to cryptographic security 19
3.3 Definitions and abbreviated terms related to the Galois/Counter Mode 29
3.4 General abbreviated terms 30
3.5 Symbols related to the Galois/Counter Mode 34
3.6 Symbols related the ECDSA algorithm 35
3.7 Symbols related to the key agreement algorithms 35
4 Overview of DLMS/COSEM 35
4.1 Information exchange in DLMS/COSEM 35
4.1.1 General 35
4.1.2 Communication model 36
4.1.3 Naming and addressing 37
4.1.4 Connection oriented operation 40
4.1.5 Application associations 41
4.1.6 Messaging patterns 42
4.1.7 Data exchange between third parties and DLMS/COSEM servers 43
4.1.8 Communication profiles 43
4.1.9 Model of a DLMS/COSEM metering system 45
4.1.10 Model of DLMS/COSEM servers 45
4.1.11 Model of a DLMS/COSEM client 47
4.1.12 Interoperability and interconnectivity in DLMS/COSEM 48
4.1.13 Ensuring interconnectivity: the protocol identification service 48
4.1.14 System integration and meter installation 49
4.2 DLMS/COSEM application layer main features 49
4.2.1 General 49
4.2.2 DLMS/COSEM application layer structure 49
4.2.3 The Association Control Service Element, ACSE 51
4.2.4 The xDLMS application service element 52
4.2.5 Layer management services 59
4.2.6 Summary of DLMS/COSEM application layer services 59
4.2.7 DLMS/COSEM application layer protocols 60
5 Information security in DLMS/COSEM 60
5.1 Overview 60
5.2 The DLMS/COSEM security concept 61
5.2.1 Overview 61
5.2.2 Identification and authentication 61
5.2.3 Security context 64
5.2.4 Access rights 64
5.2.5 Application layer message security 64
5.2.6 COSEM data security 66
5.3 Cryptographic algorithms 67

5.3.1 Overview 67
5.3.2 Hash function 67
5.3.3 Symmetric key algorithms 68
5.3.4 Public key algorithms 74
5.3.5 Random number generation 85
5.3.6 Compression 86
5.3.7 Security suite 86
5.4 Cryptographic keys – overview 87
5.5 Key used with symmetric key algorithms 87
5.5.1 Symmetric keys types 87
5.5.2 Key information with general-ciphering APDU and data protection 88
5.5.3 Key identification 89
5.5.4 Key wrapping 89
5.5.5 Key agreement 90
5.5.6 Symmetric key cryptoperiods 90
5.6 Keys used with public key algorithms 91
5.6.1 Overview 91
5.6.2 Key pair generation 91
5.6.3 Public key certificates and infrastructure 92
5.6.4 Certificate and certificate extension profile 95
5.6.5 Suite B end entity certificate types to be supported by DLMS/COSEM servers 103
5.6.6 Management of certificates 103
5.7 Applying cryptographic protection 108
5.7.1 Overview 108
5.7.2 Protecting xDLMS APDUs 108
5.7.3 Multi-layer protection by multiple parties 121
5.7.4 HLS authentication mechanisms 122
5.7.5 Protecting COSEM data 125
6 DLMS/COSEM application layer service specification 126
6.1 Service primitives and parameters 126
6.2 The COSEM-OPEN service 128
6.3 The COSEM-RELEASE service 133
6.4 COSEM-ABORT service 136
6.5 Protection and general block transfer parameters 136
6.6 The GET service 141
6.7 The SET service 144
6.8 The ACTION service 148
6.9 The ACCESS service 151
6.9.1 Overview – Main features 151
6.9.2 Service specification 153
6.10 The DataNotification service 158
6.11 The EventNotification service 159
6.12 The TriggerEventNotificationSending service 160
6.13 Variable access specification 161
6.14 The Read service 161
6.15 The Write service 165
6.16 The UnconfirmedWrite service 168
6.17 The InformationReport service 170

6.18 Client side layer management services: the SetMapperTable.request 171
6.19 Summary of services and LN/SN data transfer service mapping 171
7 DLMS/COSEM application layer protocol specification 173
7.1 The control function 173
7.1.1 State definitions of the client side control function 173
7.1.2 State definitions of the server side control function 174
7.2 The ACSE services and APDUs 175
7.2.1 ACSE functional units, services and service parameters 175
7.2.2 Registered COSEM names 179
7.2.3 APDU encoding rules 182
7.2.4 Protocol for application association establishment 182
7.2.5 Protocol for application association release 187
7.3 Protocol for the data transfer services 191
7.3.1 Negotiation of services and options – the conformance block 191
7.3.2 Confirmed and unconfirmed service invocations 192
7.3.3 Protocol for the GET service 193
7.3.4 Protocol for the SET service 197
7.3.5 Protocol for the ACTION service 200
7.3.6 Protocol for the ACCESS service 202
7.3.7 Protocol of the DataNotification service 204
7.3.8 Protocol for the EventNotification service 204
7.3.9 Protocol for the Read service 204
7.3.10 Protocol for the Write service 208
7.3.11 Protocol for the UnconfirmedWrite service 213
7.3.12 Protocol for the InformationReport service 214
7.3.13 Protocol of general block transfer mechanism 215
8 Abstract syntax of ACSE and COSEM APDUs 226
9 COSEM APDU XML schema 239
9.1 General 239
9.2 XML Schema 240
Annex A (normative) Using the DLMS/COSEM application layer in various communications profiles 261
A.1 General 261
A.2 Targeted communication environments 261
A.3 The structure of the profile 261
A.4 Identification and addressing schemes 261
A.5 Supporting layer services and service mapping 262
A.6 Communication profile specific parameters of the COSEM AL services 262
A.7 Specific considerations / constraints using certain services within a given profile 262
A.8 The 3-layer, connection-oriented, HDLC based communication profile 262
A.9 The TCP-UDP/IP based communication profiles (COSEM_on_IP) 262
A.10 The wired and wireless M-Bus communication profiles 262
A.11 The S-FSK PLC profile 262
Annex B (normative) SMS short wrapper 263
Annex C (normative) Gateway protocol 264
C.1 General 264
C.2 The gateway protocol 265
C.3 HES in the WAN/NN acting as Initiator (Pull operation) 266

C.4 End devices in the LAN acting as Initiators (Push operation) 267
C.4.1 General 267
C.4.2 End device with WAN/NN knowledge 267
C.4.3 End devices without WAN/NN knowledge 268
C.5 Security 268
Annex D (informative) AARQ and AARE encoding examples 269
D.1 General 269
D.2 Encoding of the xDLMS InitiateRequest / InitiateResponse APDU 269
D.3 Specification of the AARQ and AARE APDUs 272
D.4 Data for the examples 273
D.5 Encoding of the AARQ APDU 274
D.6 Encoding of the AARE APDU 277
Annex E (informative) Encoding examples: AARQ and AARE APDUs using a ciphered application context 283
E.1 A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key 283
E.2 Authenticated encryption of the xDLMS InitiateRequest APDU 284
E.3 The AARQ APDU 285
E.4 A-XDR encoding of the xDLMS InitiateResponse APDU 287
E.5 Authenticated encryption of the xDLMS InitiateResponse APDU 288
E.6 The AARE APDU 289
E.7 The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU) 291
E.8 The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU) 292
Annex F (informative) Data transfer service examples 293
F.1 GET / Read, SET / Write examples 293
F.2 ACCESS service example 310
F.3 Compact array encoding example 311
F.3.1 General 311
F.3.2 The specification of compact-array 311
F.3.3 Example 1: Compact array encoding an array of five long-unsigned values 313
F.3.4 Example 2: Compact-array encoding of five octet-string values 314
F.3.5 Example 3: Encoding of the buffer of a Profile generic object 314
Annex G (normative) NSA Suite B elliptic curves and domain parameters 317
Annex H (informative) Example of an End entity signature certificate using P-256 signed with P-256 319
Annex I (normative) Use of key agreement schemes in DLMS/COSEM 321
I.1 Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme 321
I.2 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme 324
I.3 Static Unified Model C(0e, 2s, ECC CDH) scheme 329
Annex J (informative) Exchanging protected xDLMS APDUs between TP and server 333
J.1 General 333
J.2 Example 1: Protection is the same in the two directions 333
J.3 Example 2: Protection is different in the two directions 334
Annex K (informative) Significant technical changes with respect to IEC 62056-5-3:2016 336
Bibliography 339
Index 343

Figure 1 – Client–server model and communication protocols 37
Figure 2 – Naming and addressing in DLMS/COSEM 38
Figure 3 – A complete communication session in the CO environment 40
Figure 4 – DLMS/COSEM messaging patterns 43
Figure 5 – DLMS/COSEM generic communication profile 44
Figure 6 – Model of a DLMS/COSEM metering system 45
Figure 7 – DLMS/COSEM server model 46
Figure 8 – Model of a DLMS/COSEM client using multiple protocol stacks 47
Figure 9 – The structure of the DLMS/COSEM application layers 50
Figure 10 – The concept of composable xDLMS messages 57
Figure 11 – Summary of DLMS/COSEM AL services 60
Figure 12 – Authentication mechanisms 62
Figure 13 – Client – server message security concept 65
Figure 14 – End-to-end message security concept 66
Figure 15 – Hash function 68
Figure 16 – Encryption and decryption 69
Figure 17 – Message Authentication Codes (MACs) 70
Figure 18 – GCM functions 71
Figure 19 – Digital signatures 78
Figure 20 – C(2e, 0s) scheme: each party contributes only an ephemeral key pair 79
Figure 21 – C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair 81
Figure 22 – C(0e, 2s) scheme: each party contributes only< a static key pair 83
Figure 23 – Architecture of a Public Key Infrastructure (example) 94
Figure 24 – MSC for provisioning the server with CA certificates 104
Figure 25 – MSC for security personalisation of the server 105
Figure 26 – Provisioning the server with the certificate of the client 106
Figure 27 – Provisioning the client / third party with a certificate of the server 107
Figure 28 – Remove certificate from the server 107
Figure 29 – Cryptographic protection of information using AES-GCM 111
Figure 30 – Structure of service-specific global / dedicated ciphering xDLMS APDUs 113
Figure 31 – Structure of general-glo-ciphering and general-ded-ciphering xDLMS APDUs 114
Figure 32 – Structure of general-ciphering xDLMS APDUs 115
Figure 33 – Structure of general-signing APDUs 121
Figure 34 – Service primitives 126
Figure 35 – Time sequence diagrams 127
Figure 36 – Additional service parameters to control cryptographic protection and GBT 137
Figure 37 – Partial state machine for the client side control function 173
Figure 38 – Partial state machine for the server side control function 174
Figure 39 – MSC for successful AA establishment preceded by a successful lower layer connection establishment 184
Figure 40 – Graceful AA release using the A-RELEASE service 189
Figure 41 – Graceful AA release by disconnecting the supporting layer 190

Figure 42 – Aborting an AA following a PH-ABORT.indication 191
Figure 43 – MSC of the GET service 194
Figure 44 – MSC of the GET service with block transfer 195
Figure 45 – MSC of the GET service with block transfer, long GET aborted 197
Figure 46 – MSC of the SET service 198
Figure 47 – MSC of the SET service with block transfer 198
Figure 48 – MSC of the ACTION service 200
Figure 49 – MSC of the ACTION service with block transfer 202
Figure 50 – ACCESS Service with long response 203
Figure 51 – ACCESS Service with long request and response 203
Figure 52 – MSC of the Read service used for reading an attribute 207
Figure 53 – MSC of the Read service used for invoking a method 207
Figure 54 – MSC of the Read service used for reading an attribute, with block transfer 208
Figure 55 – MSC of the Write service used for writing an attribute 211
Figure 56 – MSC of the Write service used for invoking a method 212
Figure 57 – MSC of the Write service used for writing an attribute, with block transfer 213
Figure 58 – MSC of the UnconfirmedWrite service used for writing an attribute 214
Figure 59 – Partial service invocations and GBT APDUs 217
Figure 60 – GET service with GBT, switching to streaming 219
Figure 61 – GET service with partial invocations, GBT and streaming, recovery of 4th block sent in the 2nd stream 220
Figure 62 – GET service with partial invocations, GBT and streaming, recovery of 4th and 5th block 221
Figure 63 – GET service with partial invocations, GBT and streaming, recovery of last block 222
Figure 64 – SET service with GBT, with server not supporting streaming, recovery of 3rd block 223
Figure 65 – ACTION-WITH-LIST service with bi-directional GBT and block recovery 224
Figure 66 – DataNotification service with GBT with partial invocation 225
Figure B.1 – Short wrapper 263
Figure C.1 – General architecture with gateway 264
Figure C.2 – The fields used for pre-fixing the COSEM APDUs 265
Figure C.3 – Pull message sequence chart 266
Figure C.4 – Push message sequence chart 267
Figure I.1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme 321
Figure I.2 – Ciphered xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme 325
Figure I.3 – Ciphered xDLMS APDU protected by an ephemeral key established using the Static Unified Model C(0e, 2s, ECC CDH) scheme 330
Figure J.1 – Exchanging protected xDLMS APDUs between TP and server: example 1 334
Figure J.2 – Exchanging protected xDLMS APDUs between TP and server: example 2 335

Table 1 – Client and server SAPs 39
Table 2 – Clarification of the meaning of PDU size for DLMS/COSEM 58

Table 3 – Elliptic curves in DLMS/COSEM security suites 76
Table 4 – Ephemeral Unified Model key agreement scheme summary 80
Table 5 – One-pass Diffie-Hellman key agreement scheme summary 82
Table 6 – Static Unified Model key agreement scheme summary 84
Table 7 – *OtherInfo* subfields and substrings 85
Table 8 – Cryptographic algorithm ID-s 85
Table 9 – DLMS/COSEM security suites 86
Table 10 – Symmetric keys types 88
Table 11 – Key information with general-ciphering APDU and data protection 89
Table 12 – Asymmetric keys types and their use 91
Table 13 – X.509 v3 Certificate structure 95
Table 14 – X.509 v3 tbsCertificate fields 96
Table 15 – Naming scheme for the Root-CA instance (informative) 97
Table 16 – Naming scheme for the Sub-CA instance (informative) 97
Table 17 – Naming scheme for the end entity instance 98
Table 18 – X.509 v3 Certificate extensions 100
Table 19 – Key Usage extensions 101
Table 20 – Subject Alternative Name values 101
Table 21 – Issuer Alternative Name values 102
Table 22 – Basic constraints extension values 102
Table 23 – Certificates handled by DLMS/COSEM end entities 103
Table 24 – Security policy values (“Security setup” version 1) 108
Table 25 – Access rights values (“Association LN” ver 3 “Association SN” ver 4) 109
Table 26 – Ciphered xDLMS APDUs 110
Table 27 – Security control byte 112
Table 28 – Plaintext and Additional Authenticated Data 112
Table 29 – Use of the fields of the ciphering xDLMS APDUs 116
Table 30 – Example: glo-get-request xDLMS APDU 117
Table 31 – ACCESS service with general-ciphering, One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) key agreement scheme 119
Table 32 – DLMS/COSEM HLS authentication mechanisms 123
Table 33 – HLS example using authentication-mechanism 5 with GMAC 124
Table 34 – HLS example using authentication-mechanism 7 with ECDSA 125
Table 35 – Codes for AL service parameters 128
Table 36 – Service parameters of the COSEM-OPEN service primitives 129
Table 37 – Service parameters of the COSEM-RELEASE service primitives 133
Table 38 – Service parameters of the COSEM-ABORT service primitives 136
Table 39 – Additional service parameters 138
Table 40 – Security parameters 139
Table 41 – APDUs used with security protection types 140
Table 42 – Service parameters of the GET service 142
Table 43 – GET service request and response types 143
Table 44 – Service parameters of the SET service 145

Table 45 – SET service request and response types 146
Table 46 – Service parameters of the ACTION service 148
Table 47 – ACTION service request and response types 149
Table 48 – Service parameters of the ACCESS service 155
Table 49 – Service parameters of the DataNotification service primitives 158
Table 50 – Service parameters of the EventNotification service primitives 159
Table 51 – Service parameters of the TriggerEventNotificationSending.request service primitive 160
Table 52 – Variable Access Specification 161
Table 53 – Service parameters of the Read service 162
Table 54 – Use of the Variable_Access_Specification variants and the Read.response choices 163
Table 55 – Service parameters of the Write service 166
Table 56 – Use of the Variable_Access_Specification variants and the Write.response choices 167
Table 57 – Service parameters of the UnconfirmedWrite service 169
Table 58 – Use of the Variable_Access_Specification variants 169
Table 59 – Service parameters of the InformationReport service 170
Table 60 – Service parameters of the SetMapperTable.request service primitives 171
Table 61 – Summary of ACSE services 171
Table 62 – Summary of xDLMS services 172
Table 63 – Functional Unit APDUs and their fields 177
Table 64 – COSEM application context names 180
Table 65 – COSEM authentication mechanism names 181
Table 66 – Cryptographic algorithm ID-s 182
Table 67 – xDLMS Conformance block 192
Table 68 – GET service types and APDUs 194
Table 69 – SET service types and APDUs 197
Table 70 – ACTION service types and APDUs 200
Table 71 – Mapping between the GET and the Read services 205
Table 72 – Mapping between the ACTION and the Read services 206
Table 73 – Mapping between the SET and the Write services *(1 of 2)* 209
Table 74 – Mapping between the ACTION and the Write service 210
Table 75 – Mapping between the SET and the UnconfirmedWrite services 214
Table 76 – Mapping between the ACTION and the UnconfirmedWrite services 214
Table 77 – Mapping between the EventNotification and InformationReport services 215
Table B.1 – Reserved Application Processes 263
Table D.1 – Conformance block 270
Table D.2 – A-XDR encoding of the xDLMS InitiateRequest APDU 271
Table D.3 – A-XDR encoding of the xDLMS InitiateResponse APDU 272
Table D.4 – BER encoding of the AARQ APDU 275
Table D.5 – Complete AARQ APDU 277
Table D.6 – BER encoding of the AARE APDU 278
Table D.7 – The complete AARE APDU 282

Table E.1 – A-XDR encoding of the xDLMS InitiateRequest APDU 284
Table E.2 – Authenticated encryption of the xDLMS InitiateRequest APDU 285
Table E.3 – BER encoding of the AARQ APDU 286
Table E.4 – A-XDR encoding of the xDLMS InitiateResponse APDU 288
Table E.5 – Authenticated encryption of the xDLMS InitiateResponse APDU 289
Table E.6 – BER encoding of the AARE APDU 290
Table E.7 – BER encoding of the RLRQ APDU 291
Table E.8 – BER encoding of the RLRE APDU 292
Table F.1 – The objects used in the examples 293
Table F.2 – Example: Reading the value of a single attribute without block transfer 294
Table F.3 – Example: Reading the value of a list of attributes without block transfer 295
Table F.4 – Example: Reading the value of a single attribute with block transfer 297
Table F.5 – Example: Reading the value of a list of attributes with block transfer 299
Table F.6 – Example: Writing the value of a single attribute without block transfer 302
Table F.7 – Example: Writing the value of a list of attributes without block transfer 303
Table F.8 – Example: Writing the value of a single attribute with block transfer 305
Table F.9 – Example: Writing the value of a list of attributes with block transfer 307
Table F.10 – Example: ACCESS service without block transfer 310
Table G.1 – ECC_P256_Domain_Parameters 317
Table G.2 – ECC_P384_Domain_Parameters 318
Table I.1 – Test vector for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme 323
Table I.2 – Test vector for key agreement using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme 327
Table I.3 – Test vector for key agreement using the Static-Unified Model (0e, 2s, ECC CDH) scheme 331

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.

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:

DLMS[1] User Association
Zug/Switzerland
www.dlms.com

_____

[1] Device Language Message Specification.

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

This third edition cancels and replaces the second edition of IEC 62056-5-3, published in 2016. It 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:

FDIS	Report on voting
13/1744/FDIS	13/1747/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

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 publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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 third edition of IEC 62056-5-3 has been prepared by IEC TC13 WG14 with a significant contribution of the DLMS User Association, its D-type liaison partner.

This edition is in line with DLMS UA 1000-2, the “Green Book” Ed. 8.2:2017. The main new features are the ACCESS service, the new security suites 1 and 2 supporting symmetric key and public key cryptography, the general protection mechanism and the XML schema for COSEM APDUs.

Clause 5 is based on parts of NIST documents. Reprinted courtesy of the National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.

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 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 edition of the standard.

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 protocol – 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 62056-6-2:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*

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

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

ISO/IEC 8825-1:2015, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 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.

ITU-T V.44: 2000 , *Series v: data communication over the telephone network – Error control – V.44:2000, Data compression procedures*

ITU-T X.509:2008, *Series x: data networks, open system communications and security – Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

ITU-T X.693 (11/2008), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

ITU-T X.693 Corrigendum 1 (10/2011), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1*

ITU-T X.694 (11/2008), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*

ITU-T X.694 Corrigendum 1 (10/2011), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical Corrigendum 1*

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

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

FIPS PUB 197:2001, *Advanced Encryption Standard (AES)*

NIST SP 800-21:2005, *Guideline for Implementing Cryptography in the Federal Government*

NIST SP 800-32:2001, *Introduction to Public Key Technology and the Federal PKI Infrastructure*

NIST SP 800-38D:2007, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

NIST SP 800-56A Rev. 2: 2013, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

NIST SP 800-57:2012, *Recommendation for Key Management – Part 1: General (Revision 3)*

NSA1, *Suite B Implementer's Guide to FIPS 186-3 (ECDSA)*, Feb 3rd 2010

NSA2, *Suite B Implementer's Guide to NIST SP800-56A*, 28th July 2009

NSA3, *NSA Suite B Base Certificate and CRL Profile*, 27th May 2008

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 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