IEC 62056-5-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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 978-2-8322-5555-1

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 176
7.2.1 ACSE functional units, services and service parameters 176
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 188
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 215
7.3.13 Protocol of general block transfer mechanism 215
8 Abstract syntax of ACSE and COSEM APDUs 226
9 COSEM APDU XML schema 240
9.1 General 240
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 325
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 338
Index 342

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 175
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 59

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).

This bilingual version (2018-04) corresponds to the English version, published in 2017-08.

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.

The French version of this standard has not been voted upon.

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.

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

SOMMAIRE

AVANT-PROPOS 358
INTRODUCTION 360
1 Domaine d'application 361
2 Références normatives 361
3 Termes, définitions, abréviations et symboles 363
3.1 Définitions générales concernant DLMS/COSEM 363
3.2 Définitions liées à la sécurité chiffrée 366
3.3 Définitions et abréviations liées au mode Galois/Counter 377
3.4 Abréviations générales 378
3.5 Symboles liés au mode Galois/Counter 382
3.6 Symboles liés à l'algorithme ECDSA 383
3.7 Symboles liés aux algorithmes à agrément de clé 383
4 Aperçu de DLMS/COSEM 384
4.1 Échange d'informations dans DLMS/COSEM 384
4.1.1 Généralités 384
4.1.2 Modèle de communication 384
4.1.3 Dénomination et adressage 386
4.1.4 Opération orientée connexion 389
4.1.5 Associations d'applications 390
4.1.6 Types de messageries 392
4.1.7 Échange de données entre des tierces parties et des serveurs DLMS/COSEM 393
4.1.8 Profils de communication 393
4.1.9 Modèle de système de comptage DLMS/COSEM 396
4.1.10 Modèle de serveurs DLMS/COSEM 396
4.1.11 Modèle d'un client DLMS/COSEM 399
4.1.12 Interopérabilité et interconnectivité dans DLMS/COSEM 401
4.1.13 Garantie de l'interconnectivité: service d'identification de protocole 402
4.1.14 Intégration de système et installation de comptage 402
4.2 Caractéristiques principales de la couche application DLMS/COSEM 403
4.2.1 Généralités 403
4.2.2 Structure de la couche application DLMS/COSEM 403
4.2.3 L'élément de service de contrôle d'association, ACSE 406
4.2.4 Élément de service d'application xDLMS 407
4.2.5 Services de gestion de couche 414
4.2.6 Récapitulatif des services de la couche application DLMS/COSEM 414
4.2.7 Protocoles de la couche application DLMS/COSEM 415
5 Sécurité des informations dans DLMS/COSEM 416
5.1 Aperçu 416
5.2 Concept de sécurité DLMS/COSEM 416
5.2.1 Aperçu 416
5.2.2 Identification et authentification 416
5.2.3 Contexte de sécurité 421
5.2.4 Droits d'accès 421
5.2.5 Sécurité des messages de la couche application 421
5.2.6 Sécurité des données COSEM 424
5.3 Algorithmes cryptographiques 424

5.3.1 Aperçu 424
5.3.2 Fonction de hachage 425
5.3.3 Algorithmes à clé symétrique 426
5.3.4 Algorithmes à clé publique 433
5.3.5 Génération de nombres aléatoires 446
5.3.6 Compression 446
5.3.7 Suite de sécurité 446
5.4 Clés cryptographiques – aperçu 447
5.5 Clés utilisées avec des algorithmes à clé symétrique 447
5.5.1 Types de clés symétriques 447
5.5.2 Informations relatives aux clés avec APDU general-ciphering et protection des données 450
5.5.3 Identification de clé 451
5.5.4 Enveloppement de clé 451
5.5.5 Agrément de clé 451
5.5.6 Périodes cryptographiques à clé symétrique 452
5.6 Clés utilisées avec des algorithmes à clé publique 452
5.6.1 Aperçu 452
5.6.2 Génération de paires de clés 453
5.6.3 Certificats de clé publique et infrastructure à clé publique 453
5.6.4 Certificat et profil d'extension de certificat 456
5.6.5 Types de certificats d'entités finales de la Suite B à prendre en charge par les serveurs DLMS/COSEM 464
5.6.6 Gestion des certificats 465
5.7 Application de la protection cryptographique 470
5.7.1 Aperçu 470
5.7.2 Protection des APDU xDLMS 470
5.7.3 Protection multicouche par plusieurs parties 487
5.7.4 Mécanismes d'authentification HLS 487
5.7.5 Protection des données COSEM 490
6 Spécification de service de la couche application DLMS/COSEM 491
6.1 Primitives de service et paramètres 491
6.2 Service COSEM-OPEN 494
6.3 Service COSEM-RELEASE 499
6.4 Service COSEM-ABORT 502
6.5 Paramètres de protection et de transfert général de blocs 503
6.6 Service GET 509
6.7 Service SET 512
6.8 Service ACTION 516
6.9 Service ACCESS 519
6.9.1 Aperçu – Principales fonctionnalités 519
6.9.2 Spécification de service 521
6.10 Service DataNotification 526
6.11 Service EventNotification 527
6.12 Service TriggerEventNotificationSending 528
6.13 Spécification d'accès variable 529
6.14 Service Read 530
6.15 Service Write 534
6.16 Service UnconfirmedWrite 537

6.17 Service InformationReport 539
6.18 Services de gestion de couches côté client: Demande SetMapperTable.request 540
6.19 Récapitulatif des services et de la mise en correspondance de services de transfert de données LN/SN 540
7 Spécification du protocole de couche application DLMS/COSEM 541
7.1 Fonction de commande 541
7.1.1 Définitions des états de la fonction de commande côté client 541
7.1.2 Définitions des états de la fonction de commande côté serveur 543
7.2 Services ACSE et APDU 544
7.2.1 Unités fonctionnelles ACSE, services et paramètres de service 544
7.2.2 Noms COSEM enregistrés 547
7.2.3 Règles de codage d'APDU 550
7.2.4 Protocole d'établissement d'association d'applications 550
7.2.5 Protocole de libération d'association d'applications 556
7.3 Protocole des services de transfert de données 562
7.3.1 Négociation de services et d'options – Bloc de conformité 562
7.3.2 Appels de service confirmés et non confirmés 563
7.3.3 Protocole du service GET 564
7.3.4 Protocole du service SET 569
7.3.5 Protocole du service ACTION 572
7.3.6 Protocole du service ACCESS 575
7.3.7 Protocole du service DataNotification 576
7.3.8 Protocole du service EventNotification 577
7.3.9 Protocole du service Read 577
7.3.10 Protocole du service Write 583
7.3.11 Protocole du service UnconfirmedWrite 588
7.3.12 Protocole du service InformationReport 589
7.3.13 Protocole du mécanisme de transfert général de blocs 590
8 Syntaxe abstraite des APDU ACSE et COSEM 605
9 Schéma XML des APDU COSEM 618
9.1 Généralités 618
9.2 Schéma XML 619
Annexe A (normative) Utilisation de la couche application DLMS/COSEM dans différents profils de communication 640
A.1 Généralités 640
A.2 Environnements de communication ciblés 640
A.3 Structure du profil 640
A.4 Schémas d'identification et d'adressage 640
A.5 Services de couche de support et mise en correspondance de services 641
A.6 Paramètres spécifiques au profil de communication des services d'AL COSEM 641
A.7 Considérations / contraintes spécifiques à l'utilisation de certains services dans un profil donné 641
A.8 Profil de communication à 3 couches, orienté connexion et basé sur HDLC 641
A.9 Profils de communication basés sur TCP-UDP/IP (COSEM_on_IP) 641
A.10 Profils de communication M-Bus câblés et sans fil 641
A.11 Profil CPL S-FSK 641

Annexe B (normative) Couche d'adaptation réduite pour SMS 642
Annexe C (normative) Protocole passerelle 643
C.1 Généralités 643
C.2 Protocole passerelle 644
C.3 HES dans le WAN/NN agissant comme Initiator (initiateur; Opération Pull) 645
C.4 Dispositifs finaux dans le LAN agissant comme Initiators (initiateurs, opération Push) 646
C.4.1 Généralités 646
C.4.2 Dispositif final ayant des connaissances sur le WAN/NN 647
C.4.3 Dispositifs finaux sans connaissances sur le WAN/NN 648
C.5 Sécurité 648
Annexe D (informative) Exemples de codages AARQ et AARE 649
D.1 Généralités 649
D.2 Codage des APDU xDLMS InitiateRequest/InitiateResponse 649
D.3 Spécification des APDU AARQ et AARE 652
D.4 Données pour les exemples 653
D.5 Codage de l'APDU AARQ 654
D.6 Codage de l'APDU AARE 657
Annexe E (informative) Exemples de codages: APDU AARQ et AARE utilisant un contexte d'application crypté 663
E.1 Codage A-XDR de l'APDU xDLMS InitiateRequest contenant une clé dédiée 663
E.2 Chiffrement authentifié de l'APDU xDLMS InitiateRequest 664
E.3 APDU AARQ 665
E.4 Codage A-XDR de l'APDU xDLMS InitiateResponse 667
E.5 Chiffrement authentifié de l'APDU xDLMS InitiateResponse 668
E.6 APDU AARE 669
E.7 APDU RLRQ (contenant une APDU xDLMS InitiateRequest chiffrée) 671
E.8 APDU RLRE (contenant une APDU xDLMS InitiateResponse chiffrée) 671
Annexe F (informative) Exemples de services de transfert de données 673
F.1 Exemples GET / Read, SET / Write 673
F.2 Exemple de service ACCESS 690
F.3 Exemple de codage compact-array 691
F.3.1 Généralités 691
F.3.2 Spécification de compact-array 691
F.3.3 Exemple 1: Codage compact-array d'un array de cinq valeurs long-unsigned 693
F.3.4 Exemple 2: Codage compact-array de cinq valeurs octet-string 694
F.3.5 Exemple 3: Codage du tampon d'un objet générique Profile (profil) 695
Annexe G (normative) Courbes elliptiques et paramètres de domaine de la Suite B NSA 698
Annexe H (informative) Exemple de certificat de signature d'entité finale utilisant P-256 signé avec P-256 700
Annexe I (normative) Utilisation des mécanismes d'agrément de clé dans DLMS/COSEM 702
I.1 Schéma Ephemeral Unified Model C(2e, 0s, ECC CDH) 702
I.2 Schéma Diffie-Hellman en une passe C(1e, 1s, ECC CDH) 705
I.3 Schéma de modèle unifié statique C(0e, 2s, ECC CDH) 710

Annexe J (informative) Échange d'APDU xDLMS protégées entre TP et serveur 715
J.1 Généralités 715
J.2 Exemple 1: Protection similaire dans les deux sens 715
J.3 Exemple 2: Protection différente dans les deux sens 717
Annexe K (informative) Modifications techniques majeures par rapport à l'IEC 62056-5-3:2016 720
Bibliographie 723
Index 727

Figure 1 – Modèle client–serveur et protocoles de communication 386
Figure 2 – Dénomination et adressage dans DLMS/COSEM 387
Figure 3 – Session complète de communication dans l'environnement CO 390
Figure 4 – Types de messageries DLMS/COSEM 393
Figure 5 – Profil générique de communication DLMS/COSEM 395
Figure 6 – Modèle de système de comptage DLMS/COSEM 396
Figure 7 – Modèle de serveur DLMS/COSEM 399
Figure 8 – Modèle de client DLMS/COSEM utilisant plusieurs piles de protocoles 401
Figure 9 – Structure des couches d'application DLMS/COSEM 405
Figure 10 – Concept de messages xDLMS composables 412
Figure 11 – Récapitulatif des services de l'AL DLMS/COSEM 415
Figure 12 – Mécanismes d'authentification 419
Figure 13 – Conception de sécurité des messages client-serveur 422
Figure 14 – Concept de sécurité de bout en bout de messages 424
Figure 15 – Fonction de hachage 426
Figure 16 – Chiffrement et déchiffrement 427
Figure 17 – Codes d'authentification de message (MAC) 428
Figure 18 – Fonctions du GCM 430
Figure 19 – Signatures numériques 437
Figure 20 – Schéma C(2e, 0s): chaque partie apporte uniquement une paire de clés éphémères 439
Figure 21 – Schémas C(1e, 1s): la partie U apporte une paire de clés éphémères, et la partie V apporte une paire de clés statiques 441
Figure 22 – Schéma C(0e, 2s): chaque partie apporte uniquement une paire de clés statiques 443
Figure 23 – Architecture d'une infrastructure à clé publique (exemple) 456
Figure 24 – MSC pour l'approvisionnement du serveur en certificats de la CA 466
Figure 25 – MSC pour la personnalisation de sécurité du serveur 467
Figure 26 – Approvisionnement du serveur en certificat du client 468
Figure 27 – Approvisionnement du client/de la tierce partie en certificat du serveur 469
Figure 28 – Suppression de certificat du serveur 470
Figure 29 – Protection cryptographique des informations utilisant AES-GCM 475
Figure 30 – Structure des APDU xDLMS de chiffrement global spécifique au service / de chiffrement dédié spécifique au service 477
Figure 31 – Structure des APDU xDLMS general-glo-ciphering et general-ded-ciphering 479

Figure 32 – Structure des APDU xDLMS general-ciphering 480
Figure 33 – Structure des APDU general-signing 486
Figure 34 – Primitives de service 491
Figure 35 – Diagrammes de séquences temporelles 492
Figure 36 – Paramètres supplémentaires de service pour contrôler la protection cryptographique et le GBT 505
Figure 37 – Diagramme d'états partiel pour la fonction de commande côté client 542
Figure 38 – Diagramme d'états partiel pour la fonction de commande côté serveur 543
Figure 39 – MSC pour l'établissement réussi d'une AA précédé de l'établissement réussi d'une connexion de couche inférieure de support 553
Figure 40 – Libération d'AA sans perte de données à l'aide du service A-RELEASE 558
Figure 41 – Libération d'AA sans perte de données par déconnexion de la couche de support 560
Figure 42 – Abandon d'une AA après la primitive PH-ABORT.indication 562
Figure 43 – MSC du service GET 565
Figure 44 – MSC du service GET avec transfert de blocs 566
Figure 45 – MSC du service GET avec transfert de blocs, GET long abandonné 568
Figure 46 – MSC du service SET 570
Figure 47 – MSC du service SET avec transfert de blocs 570
Figure 48 – MSC du service ACTION 573
Figure 49 – MSC du service ACTION avec transfert de bloc 574
Figure 50 – Service ACCESS avec réponse longue 575
Figure 51 – Service ACCESS avec demande et réponse longues 576
Figure 52 – MSC du service Read utilisé pour lire un attribut 580
Figure 53 – MSC du service Read utilisé pour appeler une méthode 581
Figure 54 – MSC du service Read utilisé pour lire un attribut, avec transfert de blocs 582
Figure 55 – MSC du service Write utilisé pour écrire un attribut 586
Figure 56 – MSC du service Write utilisé pour appeler une méthode 586
Figure 57– MSC du service Write utilisé pour écrire un attribut, avec transfert de blocs 587
Figure 58 – MSC du service UnconfirmedWrite utilisé pour écrire un attribut 589
Figure 59 – Appels de service partiels et APDU GBT 592
Figure 60 – Service GET avec GBT, passage à la diffusion en flux 594
Figure 61 – Service GET avec appels partiels, GBT et diffusion en flux, récupération du 4^{e} bloc envoyé dans le deuxième flux 596
Figure 62 – Service GET avec appels partiels, GBT et diffusion en flux, récupération des 4^{e} et 5^{e} blocs 597
Figure 63 – Service GET avec appels partiels, GBT et diffusion en flux, récupération du dernier bloc 599
Figure 64 – Service SET avec GBT, avec serveur ne prenant pas en charge la diffusion en flux, récupération du 3e bloc 600
Figure 65 – Service ACTION-WITH-LIST avec GBT bidirectionnel et récupération de blocs 602
Figure 66 – Service DataNotification avec GBT, avec appel partiel 604
Figure B.1 – Couche d'adaptation réduite 642
Figure C.1 – Architecture générale avec passerelle 644
Figure C.2 – Champs utilisés pour le préfixage des APDU COSEM 644

Figure C.3 – Tableau de séquences de messages Pull 646
Figure C.4 – Tableau de séquences de messages Push 647
Figure I.1 – MSC pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH) 703
Figure I.2 – APDU xDLMS chiffrée protégée par une clé éphémère établie à l'aide d'un schéma Diffie-Hellman en une passe (1e, 1s, ECC CDH) 706
Figure I.3 –APDU xDLMS chiffrée protégée par une clé éphémère établie à l'aide du schéma de modèle unifié statique C(0e, 2s, ECC CDH) 712
Figure J.1 – Échange d'APDU xDLMS protégées entre TP et serveur: exemple 1 717
Figure J.2 – Échange d'APDU xDLMS protégées entre TP et serveur: exemple 2 719

Tableau 1 – SAP client et serveur 388
Tableau 2 – Explication de la signification des paramètres PDU Size pour DLMS/COSEM 414
Tableau 3 – Courbes elliptiques dans les suites de sécurité DLMS/COSEM 435
Tableau 4 – Récapitulatif de mécanisme d'agrément de clé Ephemeral Unified Model 440
Tableau 5 – Récapitulatif de mécanisme d'agrément de clé Diffie-Hellman en une passe 442
Tableau 6 – Récapitulatif du mécanisme d'agrément de clé du modèle unifié statique 444
Tableau 7 – Sous-champs et sous-chaînes *OtherInfo* 445
Tableau 8 – ID d'algorithmes cryptographiques 446
Tableau 9 – Suites de sécurité DLMS/COSEM 447
Tableau 10 – Types de clés symétriques 449
Tableau 11 – Informations relatives aux clés avec APDU general-ciphering et protection des données 450
Tableau 12 – Types de clés asymétriques et leur utilisation 452
Tableau 13 – Structure de certificat X.509 v3 457
Tableau 14 – Champs du tbsCertificate X.509 v3 458
Tableau 15 – Schéma de dénomination pour l'instance de la Root-CA (informatif) 459
Tableau 16 – Schéma de dénomination pour l'instance de la Sub-CA (informatif) 459
Tableau 17 – Schéma de dénomination pour l'instance de l'entité finale 459
Tableau 18 – Extensions de certificat X.509 v3 461
Tableau 19 – Extensions Key Usage 462
Tableau 20 – Valeurs Subject Alternative Name (nom alternatif d'objet) 463
Tableau 21 – Valeurs Issuer Alternative Name (nom alternatif de l'émetteur) 463
Tableau 22 – Valeurs de l'extension Basic constraints 464
Tableau 23 – Certificats traités par des entités finales DLMS/COSEM 465
Tableau 24 – Valeurs de la politique de sécurité («Security setup» version 1) 471
Tableau 25 – Valeurs des droits d'accès («Association LN» ver 3 «Association SN» ver 4) 472
Tableau 26 – APDU xDLMS chiffrées 473
Tableau 27 – Octet de contrôle de sécurité 475
Tableau 28 – Texte brut et données supplémentaires authentifiées 476
Tableau 29 – Utilisation des champs des APDU xDLMS de chiffrement 481
Tableau 30 – Exemple: APDU xDLMS glo-get-request 482

Tableau 31 – Service ACCESS avec le mécanisme d'agrément de clé Diffie-Hellman en une passe C(1e, 1s, ECC CDH) et general-ciphering 484
Tableau 32 – Mécanismes d'authentification HLS DLMS/COSEM 488
Tableau 33 – Exemple de HLS utilisant le mécanisme d'authentification 5 avec GMAC 489
Tableau 34 – Exemple de HLS utilisant le mécanisme d'authentification 7 avec ECDSA 490
Tableau 35 – Codes des paramètres de service de l'AL 493
Tableau 36 – Paramètres de service des primitives de service COSEM-OPEN 495
Tableau 37 – Paramètres de service des primitives de service COSEM-RELEASE 500
Tableau 38 – Paramètres de service des primitives de service COSEM-ABORT 503
Tableau 39 – Paramètres supplémentaires de service 505
Tableau 40 – Paramètres de sécurité 506
Tableau 41 – APDU utilisées avec les types de protections de sécurité (Security_Protection_Type) 508
Tableau 42 – Paramètres de service du service GET 510
Tableau 43 – Types de demandes et de réponses du service GET 511
Tableau 44 – Paramètres de service du service SET 513
Tableau 45 – Types de demandes et de réponses du service SET 514
Tableau 46 – Paramètres de service du service ACTION 516
Tableau 47 – Types de demandes et de réponses du service ACTION 517
Tableau 48 – Paramètres de service du service ACCESS 523
Tableau 49 – Paramètres de service des primitives de service DataNotification 526
Tableau 50 – Paramètres de service des primitives de service EventNotification 527
Tableau 51– Paramètres de service de la primitive de service TriggerEventNotificationSending.request 528
Tableau 52 – Spécification d'accès variable 529
Tableau 53 – Paramètres de service du service Read 531
Tableau 54 – Utilisation des variantes du paramètre Variable_Access_Specification et des choix de Read.response 532
Tableau 55 – Paramètres de service du service Write 535
Tableau 56 – Utilisation des variantes de Variable_Access_Specification et des choix de Write.response 536
Tableau 57 – Paramètres de service du service UnconfirmedWrite 538
Tableau 58 – Utilisation des variantes de Variable_Access_Specification 538
Tableau 59 – Paramètres de service du service InformationReport 539
Tableau 60 – Paramètres de service des primitives de service SetMapperTable.request 540
Tableau 61 – Récapitulatif des services ACSE 540
Tableau 62 – Récapitulatif des services xDLMS 541
Tableau 63 – APDU d'unité fonctionnelle et leurs champs 545
Tableau 64 – Noms de contexte d'application COSEM 549
Tableau 65 – Noms de mécanismes d'authentification COSEM 549
Tableau 66 – ID d'algorithmes cryptographiques 550
Tableau 67 – Bloc de conformité xDLMS 563
Tableau 68 – Types et APDU de service GET 565
Tableau 69 – Types et APDU de service SET 569
Tableau 70 – Types et APDU de service ACTION 572

Tableau 71 – Mise en correspondance du service GET et du service Read 578
Tableau 72 – Mise en correspondance du service ACTION et du service Read 579
Tableau 73 – Mise en correspondance du service SET et du service Write *(1 sur 2)* 583
Tableau 74 – Mise en correspondance du service ACTION et du service Write 584
Tableau 75 – Mise en correspondance du service SET et du service UnconfirmedWrite 588
Tableau 76 – Mise en correspondance du service ACTION et du service UnconfirmedWrite 588
Tableau 77 – Mise en correspondance des services EventNotification et InformationReport 590
Tableau B.1 – Processus d'application réservés 642
Tableau D.1 – Bloc de conformité 650
Tableau D.2 – Codage A-XDR de l'APDU xDLMS InitiateRequest 651
Tableau D.3 – Codage A-XDR de l'APDU xDLMS InitiateResponse 652
Tableau D.4 – Codage BER de l'APDU AARQ 655
Tableau D.5 – APDU AARQ complète 657
Tableau D.6 – Codage BER de l'APDU AARE 658
Tableau D.7 – APDU AARE complète 662
Tableau E.1 – Codage A-XDR de l'APDU xDLMS InitiateRequest 664
Tableau E.2 – Chiffrement authentifié de l'APDU xDLMS InitiateRequest 665
Tableau E.3 – Codage BER de l'APDU AARQ 666
Tableau E.4– Codage A-XDR de l'APDU xDLMS InitiateResponse 668
Tableau E.5 – Chiffrement authentifié de l'APDU xDLMS InitiateResponse 669
Tableau E.6 – Codage BER de l'APDU AARE 670
Tableau E.7 – Codage BER de l'APDU RLRQ 671
Tableau E.8 – Codage BER de l'APDU RLRE 672
Tableau F.1 – Objets utilisés dans les exemples 673
Tableau F.2 – Exemple: Lecture de la valeur d'un attribut unique sans transfert de blocs 674
Tableau F.3 – Exemple: Lecture de la valeur d'une liste d'attributs sans transfert de blocs 675
Tableau F.4 – Exemple: Lecture de la valeur d'un attribut unique avec transfert de blocs 677
Tableau F.5 – Exemple: Lecture de la valeur d'une liste d'attributs avec transfert de blocs 679
Tableau F.6 – Exemple: Écriture de la valeur d'un attribut unique sans transfert de blocs 682
Tableau F.7 – Exemple: Écriture de la valeur d'une liste d'attributs sans transfert de blocs 683
Tableau F.8 – Exemple: Écriture de la valeur d'un attribut unique avec transfert de blocs 685
Tableau F.9 – Exemple: Écriture de la valeur d'une liste d'attributs avec transfert de blocs 687
Tableau F.10 – Exemple: Service ACCESS sans transfert général de blocs 690
Tableau G.1 – ECC_P256_Domain_Parameters 698
Tableau G.2 – ECC_P384_Domain_Parameters 699

Tableau I.1 – Vecteur d'essai pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH)..... 704

Tableau I.2 – Vecteur d'essai pour agrément de clé utilisant le schéma Diffie-Hellman en une passe (1e, 1s, ECC CDH)..... 708

Tableau I.3 – Vecteur d'essai pour agrément de clé utilisant le schéma de modèle unifié statique (0e, 2s, ECC CDH)..... 713

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ÉCHANGE DES DONNÉES DE COMPTAGE DE L'ÉLECTRICITÉ – LA SUITE DLMS/COSEM –

Partie 5-3: Couche application DLMS/COSEM

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions de la présente Norme internationale peut impliquer l'utilisation d'un service de maintenance concernant la pile de protocoles sur laquelle est basée la présente norme IEC 62056-5-3.

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ce service de maintenance.

Le fournisseur du service de maintenance a donné l'assurance à l'IEC qu'il consent à fournir des services avec des demandeurs du monde entier, à des termes et conditions raisonnables et non discriminatoires. À ce propos, la déclaration du fournisseur du service de maintenance est enregistrée à l'IEC. Des informations peuvent être demandées à:

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

La Norme internationale IEC 62056-5-3 a été établie par le comité d'études 13 de l'IEC: Comptage et pilotage de l'énergie électrique.

Cette troisième édition annule et remplace la deuxième édition de l'IEC 62056-5-3 parue en 2016. Cette édition constitue une révision technique.

Les modifications techniques majeures par rapport à l'édition précédente sont énumérées à l'Annexe K (Informative).

La présente version bilingue (2018-04) correspond à la version anglaise monolingue publiée en 2017-08.

Le texte anglais de cette norme est issu des documents 13/1744/FDIS et 13/1747/RVD.

Le rapport de vote 13/1747/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62056, publiées sous le titre général *Échange des données de comptage de l'électricité – La suite DLMS/COSEM*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo «colour inside» qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

[1] Device Language Message Specification (Spécification de message de langage de dispositif).

INTRODUCTION

Cette troisième édition de l'IEC 62056-5-3 a été établie par le groupe de travail 14 du comité d'études 13 de l'IEC avec la contribution significative de la DLMS User Association, son partenaire de liaison de type D.

Cette édition est conforme à DLMS UA 1000-2, le «Green Book» Éd. 8.2:2017. Les principales nouvelles fonctions sont le service ACCESS, les nouvelles suites de sécurité 1 et 2 prenant en charge la cryptographie à clé symétrique et à clé asymétrique, le mécanisme de protection générale et le schéma XML pour les APDU COSEM.

L'Article 5 est basé sur des parties de documents du NIST. Réimprimé avec l'aimable autorisation du NIST (National Institute of Standards and Technology), Technology Administration, U.S. Department of Commerce.

ÉCHANGE DES DONNÉES DE COMPTAGE DE L'ÉLECTRICITÉ – LA SUITE DLMS/COSEM –

Partie 5-3: Couche application DLMS/COSEM

1 Domaine d'application

La présente partie de l'IEC 62056 spécifie la couche application DLMS/COSEM en termes de structure, de services et de protocoles pour les clients et serveurs DLMS/COSEM, et définit les règles de spécification des profils de communication DLMS/COSEM.

Elle définit les services permettant d'établir et de libérer des associations d'applications, ainsi que les services de communication de données permettant d'accéder aux méthodes et aux attributs des objets d'interface COSEM, définis dans l'IEC 62056-6-2, à l'aide du référencement par nom logique (LN - *logical name*) ou par nom abrégé (SN - *short name*).

L'Annexe A (normative) définit comment utiliser la couche application COSEM dans différents profils de communication. Elle indique comment différents profils de communication peuvent être construits de sorte à échanger des données avec les équipements de mesure à l'aide du modèle d'interface COSEM, ainsi que les éléments nécessaires à indiquer dans chaque profil de communication. Les profils de communication réels, spécifiques au support, sont spécifiés dans des parties distinctes de la série IEC 62056.

L'Annexe B (normative) spécifie la couche d'adaptation réduite pour SMS.

L'Annexe C (normative) spécifie le protocole passerelle.

L'Annexe D, l'Annexe E et l'Annexe F (informatives) incluent des exemples de codage d'APDU.

L'Annexe G (normative) spécifie des courbes elliptiques et des paramètres de domaine de la Suite B de la NSA.

L'Annexe H (informative) donne un exemple de certificat de signature d'entité finale utilisant P-256 signé avec P-256.

L'Annexe I (normative) spécifie l'utilisation de mécanismes d'agrément de clé dans DLMS/COSEM.

L'Annexe J (informative) donne des exemples d'échanges d'APDU xDLMS protégées entre une tierce partie et un serveur.

L'Annexe K (informative) énumère les modifications techniques majeures contenues dans la présente édition de la norme.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61334-4-41:1996, *Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4: Protocoles de communication de données – Section 41: Protocoles d'application – Spécification des messages de ligne de distribution*

IEC 61334-6:2000, *Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 6: Règles d'encodage A-XDR*

IEC TR 62051:1999, *Electricity metering – Glossary of terms* (disponible en anglais seulement)

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* (disponible en anglais seulement)

IEC 62056-6-2:2017, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 6-2: Classes d'interfaces COSEM*

IEC 62056-8-3:2013, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 8-3: Profil de communication pour réseaux de voisinage CPL S-FSK*

ISO/IEC 8824-1, *Technologies de l'information - Notation de syntaxe abstraite numéro un (ASN.1): Spécification de la notation de base*

ISO/IEC 8825-1:2015, *Technologies de l'information - Règles de codage ASN.1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)*

ISO/IEC 15953:1999, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service pour l'élément de service de contrôle d'association des objets de service d'application*

NOTE Cette norme annule et remplace l'ISO/IEC 8649:1996 et ses Amd. 1:1997 et Amd. 2:1998, dont elle constitue une révision technique.

ISO/IEC 15954:1999, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion pour l'élément de service de contrôle d'association des objets de service d'application*

NOTE Cette norme annule et remplace l'ISO/IEC 8650-1:1999 et ses Amd. 1:1997 et Amd. 2:1998, dont elle constitue une révision technique.

UIT-T V.44: 2000, *Série v: communication de données sur le réseau téléphonique – Contrôle d'erreur – V.44:2000, Procédures de compression de données*

UIT-T X.509:2008, *Série x: réseaux de données, communication entre systèmes ouverts et sécurité – Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*

UIT-T X.693 (11/2008), *Technologies de l'information – Règles de codage ASN.1: Règles de codage XML (XER)*

UIT-T X.693 Corrigendum 1 (10/2011), *Technologies de l'information – Règles de codage ASN.1: Règles de codage XML (XER) Corrigendum technique 1*

UIT-T X.694 (11/2008), *Technologies de l'information – Règles de codage ASN.1: Mappage en ASN.1 des définitions de schéma XML du W3C*

UIT-T X.694 Corrigendum 1 (10/2011), *Technologies de l'information – Règles de codage ASN.1: Mappage en ASN.1 des définitions de schéma XML du W3C Corrigendum technique 1*

FIPS PUB 180-4:2012, *Secure hash standard* (disponible en anglais seulement)

FIPS PUB 186-4:2013, *Digital Signature Standard (DSS)* (disponible en anglais seulement)

FIPS PUB 197:2001, *Advanced Encryption Standard (AES)* (disponible en anglais seulement)

NIST SP 800-21:2005, *Guideline for Implementing Cryptography in the Federal Government* (disponible en anglais seulement)

NIST SP 800-32:2001, *Introduction to Public Key Technology and the Federal PKI Infrastructure* (disponible en anglais seulement)

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

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

NIST SP 800-57:2012, *Recommendation for Key Management – Part 1:* General *(Révision 3)* (disponible en anglais seulement)

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

NSA2, *Suite B Implementer's Guide to NIST SP800-56A*, 28th July 2009 (disponible en anglais seulement)

NSA3, *NSA Suite B Base Certificate and CRL Profile*, 27th May 2008 (disponible en anglais seulement)

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 (disponible en anglais seulement)

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

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