ANSI C12/IEC 62056-5-3 ED3

American National Standard
for Electricity Metering Data Exchange – The DLMS/ COSEM Suite
Part 5-3:DLMS/COSEM Application Layer
NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

ANSI standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, express or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller’s products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEMA has no power, nor does it undertake to police or enforce compliance with the contents of this document. NEMA does not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health- or safety-related information in this document shall not be attributable to NEMA and is solely the responsibility of the certifier or maker of the statement.

© 2019 National Electrical Manufacturers Association
Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

Caution Notice: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.
FOREWORD FOR U.S. ADOPTION

This American National Standard is an adoption of IEC 62056-5-3 Ed. 3 *Electricity Metering Data Exchange – The DLMS/ COSEM Suite Part 5-3: DLMS/COSEM Application Layer*. Any reference in this standard to an IEC 62056 part is understood to mean a reference to the equivalent ANSI/IEC 62056 part, where it exists.

This standard contains all the original text from IEC 62056-5-3 Ed. 3 without change.

Suggestions for the improvement of this standard are welcome and should be submitted to:

Vice President, Technical Services
National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, VA 22209

This standard was processed and approved by committee of interested stakeholders as required by ANSI for adoption. In this particular situation, all committee members voted for its approval. At the time this standard was approved, the committee consisted of the following members:

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Name of Representative</th>
<th>Organization Represented</th>
<th>Name of Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Interest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elevate Energy</td>
<td>L. Kotewa</td>
<td>NIST</td>
<td>T. Nelson</td>
</tr>
<tr>
<td>ERCOT</td>
<td>D. Tucker</td>
<td>Power Measurements, LLC</td>
<td>W. Hardy</td>
</tr>
<tr>
<td>EnerNex LLC</td>
<td>A. Snyder</td>
<td>UL, LLC</td>
<td>S. Hunter</td>
</tr>
<tr>
<td>Future DOS R&amp;D Inc.</td>
<td>A. Moise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MET Laboratories, Inc.</td>
<td>J. Reed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aclara</td>
<td>C. Crittenden</td>
<td>Schweitzer Engineering</td>
<td>S. Nalla</td>
</tr>
<tr>
<td>Honeywell</td>
<td>M. Yarbrough</td>
<td>Sensus, A Xylem Brand</td>
<td>K. O'Dell</td>
</tr>
<tr>
<td>Itron Inc.</td>
<td>B. Cain</td>
<td>Technology for Energy Corp</td>
<td>S. Hudson</td>
</tr>
<tr>
<td>Landis+Gyr Inc.</td>
<td>J. Voisine</td>
<td>TESCO</td>
<td>T. Lawton</td>
</tr>
<tr>
<td>Milbank Manufacturing Co.</td>
<td>S. Glasgow</td>
<td>Watthour Engineering Co.</td>
<td>L. Wren</td>
</tr>
<tr>
<td>Radian Research, Inc.</td>
<td>J. Canine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>S. Pedro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alabama Power Co.</td>
<td>D. Rhoades</td>
<td>Florida Power &amp; Light</td>
<td>J. DeMars</td>
</tr>
<tr>
<td>Baltimore Gas &amp; Electric</td>
<td>J. Thurber</td>
<td>Oncor Electric Delivery Co. LLC</td>
<td>M. DeVillers</td>
</tr>
<tr>
<td>Consumers Energy</td>
<td>D. Jirikovic</td>
<td>Pacific Gas &amp; Electric</td>
<td>D. Y. Nguyen</td>
</tr>
<tr>
<td>DTE Energy</td>
<td>K. Tolios</td>
<td>Public Service Electric &amp; Gas</td>
<td>D. Ellis</td>
</tr>
<tr>
<td>Duke Energy</td>
<td>K. Barnette</td>
<td>SASK Power</td>
<td>C. Kasian</td>
</tr>
<tr>
<td>Eversource Energy</td>
<td>G. Belcher</td>
<td>Xcel Energy</td>
<td>D. Nordell</td>
</tr>
<tr>
<td>Hydro Quebec</td>
<td>J. Sabourin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOREWORD</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>1</td>
<td>Scope</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>Terms, definitions, abbreviated terms and symbols</td>
<td>19</td>
</tr>
<tr>
<td>3.1</td>
<td>General DLMS/COSEM definitions</td>
<td>19</td>
</tr>
<tr>
<td>3.2</td>
<td>Definitions related to cryptographic security</td>
<td>22</td>
</tr>
<tr>
<td>3.3</td>
<td>Definitions and abbreviated terms related to the Galois/Counter Mode</td>
<td>32</td>
</tr>
<tr>
<td>3.4</td>
<td>General abbreviated terms</td>
<td>33</td>
</tr>
<tr>
<td>3.5</td>
<td>Symbols related to the Galois/Counter Mode</td>
<td>37</td>
</tr>
<tr>
<td>3.6</td>
<td>Symbols related the ECDSA algorithm</td>
<td>38</td>
</tr>
<tr>
<td>3.7</td>
<td>Symbols related to the key agreement algorithms</td>
<td>38</td>
</tr>
<tr>
<td>4</td>
<td>Overview of DLMS/COSEM</td>
<td>38</td>
</tr>
<tr>
<td>4.1</td>
<td>Information exchange in DLMS/COSEM</td>
<td>38</td>
</tr>
<tr>
<td>4.1.1</td>
<td>General</td>
<td>38</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Communication model</td>
<td>39</td>
</tr>
<tr>
<td>4.1.3</td>
<td>Naming and addressing</td>
<td>40</td>
</tr>
<tr>
<td>4.1.4</td>
<td>Connection oriented operation</td>
<td>43</td>
</tr>
<tr>
<td>4.1.5</td>
<td>Application associations</td>
<td>44</td>
</tr>
<tr>
<td>4.1.6</td>
<td>Messaging patterns</td>
<td>45</td>
</tr>
<tr>
<td>4.1.7</td>
<td>Data exchange between third parties and DLMS/COSEM servers</td>
<td>46</td>
</tr>
<tr>
<td>4.1.8</td>
<td>Communication profiles</td>
<td>46</td>
</tr>
<tr>
<td>4.1.9</td>
<td>Model of a DLMS/COSEM metering system</td>
<td>48</td>
</tr>
<tr>
<td>4.1.10</td>
<td>Model of DLMS/COSEM servers</td>
<td>48</td>
</tr>
<tr>
<td>4.1.11</td>
<td>Model of a DLMS/COSEM client</td>
<td>50</td>
</tr>
<tr>
<td>4.1.12</td>
<td>Interoperability and interconnectivity in DLMS/COSEM</td>
<td>51</td>
</tr>
<tr>
<td>4.1.13</td>
<td>Ensuring interconnectivity: the protocol identification service</td>
<td>51</td>
</tr>
<tr>
<td>4.1.14</td>
<td>System integration and meter installation</td>
<td>52</td>
</tr>
<tr>
<td>4.2</td>
<td>DLMS/COSEM application layer main features</td>
<td>52</td>
</tr>
<tr>
<td>4.2.1</td>
<td>General</td>
<td>52</td>
</tr>
<tr>
<td>4.2.2</td>
<td>DLMS/COSEM application layer structure</td>
<td>52</td>
</tr>
<tr>
<td>4.2.3</td>
<td>The Association Control Service Element, ACSE</td>
<td>54</td>
</tr>
<tr>
<td>4.2.4</td>
<td>The xDLMS application service element</td>
<td>55</td>
</tr>
<tr>
<td>4.2.5</td>
<td>Layer management services</td>
<td>62</td>
</tr>
<tr>
<td>4.2.6</td>
<td>Summary of DLMS/COSEM application layer services</td>
<td>62</td>
</tr>
<tr>
<td>4.2.7</td>
<td>DLMS/COSEM application layer protocols</td>
<td>63</td>
</tr>
<tr>
<td>5</td>
<td>Information security in DLMS/COSEM</td>
<td>63</td>
</tr>
<tr>
<td>5.1</td>
<td>Overview</td>
<td>63</td>
</tr>
<tr>
<td>5.2</td>
<td>The DLMS/COSEM security concept</td>
<td>64</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Overview</td>
<td>64</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Identification and authentication</td>
<td>64</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Security context</td>
<td>67</td>
</tr>
</tbody>
</table>

© 2019 National Electrical Manufacturers Association
5.2.4 Access rights .........................................................................................67
5.2.5 Application layer message security ........................................................67
5.2.6 COSEM data security ...........................................................................70
5.3 Cryptographic algorithms ..........................................................................70
  5.3.1 Overview ............................................................................................70
  5.3.2 Hash function ......................................................................................70
  5.3.3 Symmetric key algorithms ...................................................................71
  5.3.4 Public key algorithms ..........................................................................77
  5.3.5 Random number generation .................................................................88
  5.3.6 Compression .........................................................................................89
  5.3.7 Security suite .......................................................................................89
5.4 Cryptographic keys – overview .................................................................90
5.5 Key used with symmetric key algorithms ..................................................90
  5.5.1 Symmetric keys types ..........................................................................90
  5.5.2 Key information with general-ciphering APDU and data protection ....91
  5.5.3 Key identification ................................................................................92
  5.5.4 Key wrapping .......................................................................................92
  5.5.5 Key agreement .....................................................................................93
  5.5.6 Symmetric key cryptoperiods .................................................................94
5.6 Keys used with public key algorithms .........................................................94
  5.6.1 Overview .............................................................................................94
  5.6.2 Key pair generation .............................................................................94
  5.6.3 Public key certificates and infrastructure .............................................95
  5.6.4 Certificate and certificate extension profile ..........................................98
  5.6.5 Suite B end entity certificate types to be supported by DLMS/COSEM
       servers .................................................................................................106
  5.6.6 Management of certificates ................................................................106
5.7 Applying cryptographic protection .............................................................111
  5.7.1 Overview ...........................................................................................111
  5.7.2 Protecting xDLMS APDUs .................................................................111
  5.7.3 Multi-layer protection by multiple parties ..........................................124
  5.7.4 HLS authentication mechanisms .......................................................125
  5.7.5 Protecting COSEM data .................................................................128
6 DLMS/COSEM application layer service specification ................................129
  6.1 Service primitives and parameters .........................................................129
  6.2 The COSEM-OPEN service ...............................................................131
  6.3 The COSEM-RELEASE service ...........................................................136
  6.4 COSEM-ABORT service ......................................................................139
  6.5 Protection and general block transfer parameters ...................................140
  6.6 The GET service ..................................................................................145
  6.7 The SET service ....................................................................................148
  6.8 The ACTION service ..........................................................................152
  6.9 The ACCESS service ..........................................................................155
    6.9.1 Overview – Main features .................................................................155
    6.9.2 Service specification .................................................................157
  6.10 The DataNotification service ..............................................................162
  6.11 The EventNotification service ............................................................163
  6.12 The TriggerEventNotificationSending service ....................................164
  6.13 Variable access specification ..............................................................165
6.14 The Read service ................................................................. 165
6.15 The Write service ............................................................... 169
6.16 The UnconfirmedWrite service ............................................ 172
6.17 The InformationReport service .......................................... 174
6.18 Client side layer management services: the SetMapperTable.request ........................................ 175
6.19 Summary of services and LN/SN data transfer service mapping .................................................. 175
7 DLMS/COSEM application layer protocol specification .......................................................... 177
  7.1 The control function .......................................................... 177
    7.1.1 State definitions of the client side control function .......... 177
    7.1.2 State definitions of the server side control function .......... 178
  7.2 The ACSE services and APDUs .......................................... 179
    7.2.1 ACSE functional units, services and service parameters .......... 179
    7.2.2 Registered COSEM names .............................................. 183
    7.2.3 APDU encoding rules .................................................... 186
    7.2.4 Protocol for application association establishment ................ 186
    7.2.5 Protocol for application association release ...................... 191
  7.3 Protocol for the data transfer services ................................ 195
    7.3.1 Negotiation of services and options – the conformance block .......... 195
    7.3.2 Confirmed and unconfirmed service invocations .................. 196
    7.3.3 Protocol for the GET service .......................................... 197
    7.3.4 Protocol for the SET service .......................................... 201
    7.3.5 Protocol for the ACTION service ..................................... 204
    7.3.6 Protocol for the ACCESS service ..................................... 206
    7.3.7 Protocol for the DataNotifcation service ......................... 208
    7.3.8 Protocol for the EventNotification service ....................... 208
    7.3.9 Protocol for the Read service ........................................ 208
    7.3.10 Protocol for the Write service ...................................... 213
    7.3.11 Protocol for the UnconfirmedWrite service ...................... 218
    7.3.12 Protocol for the InformationReport service ...................... 219
    7.3.13 Protocol of general block transfer mechanism ................... 220
8 Abstract syntax of ACSE and COSEM APDUs ............................................................... 231
9 COSEM APDU XML schema .......................................................... 245
  9.1 General ........................................................................... 245
  9.2 XML Schema ................................................................. 245
Annex A (normative) Using the DLMS/COSEM application layer in various communications profiles ........................................................................ 267
  A.1 General ........................................................................... 267
  A.2 Targeted communication environments ................................. 267
  A.3 The structure of the profile ............................................... 267
  A.4 Identification and addressing schemes ................................ 267
  A.5 Supporting layer services and service mapping ...................... 268
  A.6 Communication profile specific parameters of the COSEM AL services ........................................... 268
  A.7 Specific considerations / constraints using certain services within a given profile ......................... 268
  A.8 The 3-layer, connection-oriented, HDLC based communication profile ........................................... 268
  A.9 The TCP-UDP/IP based communication profiles (COSEM_on_IP) .................................................. 268
  A.10 The wired and wireless M-Bus communication profiles ................................................................. 268
  A.11 The S-FSK PLC profile ..................................................... 268

© 2019 National Electrical Manufacturers Association
Annex B (normative) SMS short wrapper ................................................................. 269
Annex C (normative) Gateway protocol ................................................................. 270
  C.1 General ............................................................................................................. 270
  C.2 The gateway protocol ....................................................................................... 271
  C.3 HES in the WAN/NN acting as Initiator (Pull operation) .............................. 272
  C.4 End devices in the LAN acting as Initiators (Push operation) ................. 273
    C.4.1 General ..................................................................................................... 273
    C.4.2 End device with WAN/NN knowledge .................................................... 273
    C.4.3 End devices without WAN/NN knowledge ............................................. 274
  C.5 Security ........................................................................................................... 274
Annex D (informative) AARQ and AARE encoding examples ................................ 275
  D.1 General ............................................................................................................. 275
  D.2 Encoding of the xDLMS InitiateRequest / InitiateResponse APDU .......... 275
  D.3 Specification of the AARQ and AARE APDUs ........................................... 278
  D.4 Data for the examples ..................................................................................... 279
  D.5 Encoding of the AARQ APDU ......................................................................... 280
  D.6 Encoding of the AARE APDU ......................................................................... 283
Annex E (informative) Encoding examples: AARQ and AARE APDUs using a ciphered application context................................. 289
  E.1 A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key .......................................................... 289
  E.2 Authenticated encryption of the xDLMS InitiateRequest APDU .................. 290
  E.3 The AARQ APDU ........................................................................................... 291
  E.4 A-XDR encoding of the xDLMS InitiateResponse APDU .......................... 293
  E.5 Authenticated encryption of the xDLMS InitiateResponse APDU ............ 294
  E.6 The AARE APDU ........................................................................................... 295
  E.7 The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU) ...... 297
  E.8 The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU) .... 298
Annex F (informative) Data transfer service examples ............................................... 299
  F.1 GET / Read, SET / Write examples ................................................................. 299
  F.2 ACCESS service example ............................................................................... 316
  F.3 Compact array encoding example ................................................................. 317
    F.3.1 General ...................................................................................................... 317
    F.3.2 The specification of compact-array ............................................................. 317
    F.3.3 Example 1: Compact array encoding an array of five long-unsigned values ............................................................................. 319
    F.3.4 Example 2: Compact-array encoding of five octet-string values ............ 320
    F.3.5 Example 3: Encoding of the buffer of a Profile generic object ............... 321
Annex G (normative) NSA Suite B elliptic curves and domain parameters ............ 324
Annex H (informative) Example of an End entity signature certificate using P-256 signed with P-256 ................................................................. 326
Annex I (normative) Use of key agreement schemes in DLMS/COSEM ................. 328
  I.1 Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme ............................. 328
  I.2 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme ................................ 331
  I.3 Static Unified Model C(0e, 2s, ECC CDH) scheme ....................................... 336
Annex J (informative) Exchanging protected xDLMS APDUs between TP and server .......... 340
  J.1 General .......................................................................................................... 340
  J.2 Example 1: Protection is the same in the two directions .............................. 340
Figure 1 – Client–server model and communication protocols .............................................................. 40
Figure 2 – Naming and addressing in DLMS/COSEM ........................................................................ 41
Figure 3 – A complete communication session in the CO environment ............................................. 43
Figure 4 – DLMS/COSEM messaging patterns .................................................................................. 46
Figure 5 – DLMS/COSEM generic communication profile ................................................................. 47
Figure 6 – Model of a DLMS/COSEM metering system ..................................................................... 48
Figure 7 – DLMS/COSEM server model ............................................................................................ 49
Figure 8 – Model of a DLMS/COSEM client using multiple protocol stacks ..................................... 50
Figure 9 – The structure of the DLMS/COSEM application layers ..................................................... 53
Figure 10 – The concept of composable xDLMS messages .................................................................. 60
Figure 11 – Summary of DLMS/COSEM AL services ........................................................................ 63
Figure 12 – Authentication mechanisms ............................................................................................. 65
Figure 13 – Client – server message security concept ......................................................................... 68
Figure 14 – End-to-end message security concept ............................................................................... 69
Figure 15 – Hash function .................................................................................................................. 71
Figure 16 – Encryption and decryption ................................................................................................ 72
Figure 17 – Message Authentication Codes (MACs) ........................................................................... 73
Figure 18 – GCM functions ................................................................................................................ 75
Figure 19 – Digital signatures .............................................................................................................. 81
Figure 20 – C(2e, 0s) scheme: each party contributes only an ephemeral key pair ........................... 83
Figure 21 – C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair ........................................................................................................ 84
Figure 22 – C(0e, 2s) scheme: each party contributes only< a static key pair ..................................... 86
Figure 23 – Architecture of a Public Key Infrastructure (example) ....................................................... 97
Figure 24 – MSC for provisioning the server with CA certificates ...................................................... 107
Figure 25 – MSC for security personalisation of the server ................................................................. 108
Figure 26 – Provisioning the server with the certificate of the client .................................................. 109
Figure 27 – Provisioning the client / third party with a certificate of the server ................................. 110
Figure 28 – Remove certificate from the server ................................................................................. 110
Figure 29 – Cryptographic protection of information using AES-GCM ............................................. 114
Figure 30 – Structure of service-specific global / dedicated ciphering xDLMS APDUs .................. 116
Figure 31 – Structure of general-glo-ciphering and general-ded-ciphering xDLMS APDUs .......... 117
Figure 32 – Structure of general-ciphering xDLMS APDUs ............................................................. 118
Figure 33 – Structure of general-signing APDUs .............................................................................. 124
Figure 34 – Service primitives ........................................................................................................... 129
Figure 35 – Time sequence diagrams ................................................................................................ 130
Figure 36 – Additional service parameters to control cryptographic protection and GBT ............. 141
Figure 37 – Partial state machine for the client side control function ...........................................177
Figure 38 – Partial state machine for the server side control function ...........................................178
Figure 39 – MSC for successful AA establishment preceded by a successful lower layer connection establishment ..................................................................................................................188
Figure 40 – Graceful AA release using the A-RELEASE service ......................................................193
Figure 41 – Graceful AA release by disconnecting the supporting layer ...........................................194
Figure 42 – Aborting an AA following a PH-ABORT.indication ......................................................195
Figure 43 – MSC of the GET service .................................................................................................198
Figure 44 – MSC of the GET service with block transfer .................................................................199
Figure 45 – MSC of the GET service with block transfer, long GET aborted .............................201
Figure 46 – MSC of the SET service .................................................................................................202
Figure 47 – MSC of the SET service with block transfer .................................................................202
Figure 48 – MSC of the ACTION service .........................................................................................204
Figure 49 – MSC of the ACTION service with block transfer .........................................................206
Figure 50 – ACCESS Service with long response ............................................................................207
Figure 51 – ACCESS Service with long request and response .......................................................207
Figure 52 – MSC of the Read service used for reading an attribute ................................................211
Figure 53 – MSC of the Read service used for invoking a method ..................................................211
Figure 54 – MSC of the Read service used for reading an attribute, with block transfer ............212
Figure 55 – MSC of the Write service used for writing an attribute ................................................216
Figure 56 – MSC of the Write service used for invoking a method ..................................................217
Figure 57 – MSC of the Write service used for writing an attribute, with block transfer ............218
Figure 58 – MSC of the UnconfirmedWrite service used for writing an attribute ......................219
Figure 59 – Partial service invocations and GBT APDUs ...............................................................222
Figure 60 – GET service with GBT, switching to streaming ..........................................................224
Figure 61 – GET service with partial invocations, GBT and streaming, recovery of 4th block sent in the 2nd stream ...................................................................................................................225
Figure 62 – GET service with partial invocations, GBT and streaming, recovery of 4th and 5th block ........................................................................................................................................226
Figure 63 – GET service with partial invocations, GBT and streaming, recovery of last block ........................................................................................................................................227
Figure 64 – SET service with GBT, with server not supporting streaming, recovery of 3rd block ........................................................................................................................................228
Figure 65 – ACTION-WITH-LIST service with bi-directional GBT and block recovery ............229
Figure 66 – DataNotification service with GBT with partial invocation .......................................230
Figure B.1 – Short wrapper ...............................................................................................................269
Figure C.1 – General architecture with gateway ...............................................................................270
Figure C.2 – The fields used for pre-fixing the COSEM APDUs .....................................................271
Figure C.3 – Pull message sequence chart ......................................................................................272
Figure C.4 – Push message sequence chart ....................................................................................273
Figure I.1.1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme ........................................................................................................................................328
Figure I.1.2 – Ciphered xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme ....................................................................................332
Table 37 – Static Unified Model key agreement scheme summary .......................................114
Table 36 – Elliptic curves in DLMS/COSEM security suites ........................................113
Table 35 – One-pass Diffie-Hellman key agreement scheme summary ..............................112
Table 34 – Asymmetric keys types and their use .............................................................111
Table 33 – Key information with general-ciphering APDU and data protection ..................110
Table 32 – Cryptographic algorithm ID-s ........................................................................109
Table 31 – Elliptic curves in DLMS/COSEM security suites ........................................108
Table 30 – Symmetric keys types ..................................................................................107
Table 29 – Client and server SAPs ................................................................................106
Table 28 – X.509 v3 Certificate extensions .....................................................................105
Table 27 – Key Usage extensions ..................................................................................104
Table 26 – X.509 v3 Certificate structure .......................................................................103
Table 25 – OtherInfo subfields and substrings ...............................................................102
Table 24 – Service parameters of the COSEM ..............................................................101
Table 23 – Ciphered xDLMS APDUs ............................................................................100
Table 22 – Security control byte ..................................................................................99
Table 21 – Subject Alternative Name values ..................................................................98
Table 20 – Issuer Alternative Name values .....................................................................97
Table 19 – X.509 v3 Certificate structure .......................................................................96
Table 18 – Ciphered xDLMS APDUs ............................................................................95
Table 17 – Security policy values (“Security setup” version 3) ........................................94
Table 16 – Naming scheme for the Sub-CA instance (informative) ....................................93
Table 15 – Naming scheme for the Root-CA instance (informative) ..................................92
Table 14 – DLMS/COSEM security suites ....................................................................91
Table 13 – X.509 v3 Certificate structure .......................................................................90
Table 12 – X.509 v3 Certificate structure ......................................................................89
Table 11 – Security policy values (“Security setup” version 1) ........................................88
Table 10 – Symmetric keys types ..................................................................................87
Table 9 – Static Unified Model key agreement scheme summary .....................................86
Table 8 – Cryptographic algorithm ID-s ........................................................................85
Table 7 – OtherInfo subfields and substrings ...............................................................84
Table 6 – Static Unified Model key agreement scheme summary .....................................83
Table 5 – One-pass Diffie-Hellman key agreement scheme summary ..............................82
Table 4 – Elliptic curves in DLMS/COSEM security suites ........................................181
Table 3 – One-pass Diffie-Hellman key agreement scheme summary ..............................180
Table 2 – Elliptic curves in DLMS/COSEM security suites ........................................179
Table 1 – One-pass Diffie-Hellman key agreement scheme summary ..............................178

© 2019 National Electrical Manufacturers Association
Table 38 – Service parameters of the COSEM-ABORT service primitives ............................................139
Table 39 – Additional service parameters ..................................................................................................142
Table 40 – Security parameters ..................................................................................................................143
Table 41 – APDUs used with security protection types .................................................................................144
Table 42 – Service parameters of the GET service .......................................................................................146
Table 43 – GET service request and response types .......................................................................................147
Table 44 – Service parameters of the SET service .........................................................................................149
Table 45 – SET service request and response types .......................................................................................150
Table 46 – Service parameters of the ACTION service ...............................................................................152
Table 47 – ACTION service request and response types ...............................................................................153
Table 48 – Service parameters of the ACCESS service .................................................................................159
Table 49 – Service parameters of the DataNotification service primitives .....................................................162
Table 50 – Service parameters of the EventNotification service primitives ...............................................163
Table 51 – Service parameters of the TriggerEventNotificationSending.request service primitive ..................164
Table 52 – Variable Access Specification .....................................................................................................165
Table 53 – Service parameters of the Read service .......................................................................................166
Table 54 – Use of the Variable_Access_Specification variants and the Read.response choices .......................167
Table 55 – Service parameters of the Write service .......................................................................................170
Table 56 – Use of the Variable_Access_Specification variants and the Write.response choices .......................171
Table 57 – Service parameters of the UnconfirmedWrite service ...................................................................173
Table 58 – Use of the Variable_Access_Specification variants .......................................................................173
Table 59 – Service parameters of the InformationReport service ...............................................................174
Table 60 – Service parameters of the SetMapperTable.request service primitives ........................................175
Table 61 – Summary of ACSE services ....................................................................................................175
Table 62 – Summary of xDLMS services ....................................................................................................176
Table 63 – Functional Unit APDUs and their fields ......................................................................................181
Table 64 – COSEM application context names ............................................................................................184
Table 65 – COSEM authentication mechanism names ..................................................................................185
Table 66 – Cryptographic algorithm ID-s ...................................................................................................186
Table 67 – xDLMS Conformance block .......................................................................................................196
Table 68 – GET service types and APDUs ....................................................................................................198
Table 69 – SET service types and APDUs ....................................................................................................201
Table 70 – ACTION service types and APDUs ............................................................................................204
Table 71 – Mapping between the GET and the Read services .......................................................................209
Table 72 – Mapping between the ACTION and the Read services ...............................................................210
Table 73 – Mapping between the SET and the Write services (1 of 2) ............................................................213
Table 74 – Mapping between the ACTION and the Write service ...............................................................215
Table 75 – Mapping between the SET and the UnconfirmedWrite services ................................................219
Table 76 – Mapping between the ACTION and the UnconfirmedWrite services .........................................219
Table 77 – Mapping between the EventNotification and InformationReport services ..................................220
Table B.1 – Reserved Application Processes ............................................................................................269
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 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:

<table>
<thead>
<tr>
<th>FDIS</th>
<th>Report on voting</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/1744/FDIS</td>
<td>13/1747/RVD</td>
</tr>
</tbody>
</table>

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.
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.