# IEC 62056-5-3

Edition 4.0 2023-09

# 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



IEC 62056-5-3:2023-09(en-fr)



**THIS PUBLICATION IS COPYRIGHT PROTECTED**

**Copyright © 2023 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch


**About the IEC**
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

**About IEC publications**
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

**IEC publications search - webstore.iec.ch/advsearchform**
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

**IEC Just Published - webstore.iec.ch/justpublished**
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

**IEC Customer Service Centre - webstore.iec.ch/csc**
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

**IEC Products & Services Portal - products.iec.ch**
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - www.electropedia.org**
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

---

**A propos de l'IEC**
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

**A propos des publications IEC**
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

**Recherche de publications IEC - webstore.iec.ch/advsearchform**
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

**IEC Just Published - webstore.iec.ch/justpublished**
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

**Service Clients - webstore.iec.ch/csc**
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

**IEC Products & Services Portal - products.iec.ch**
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

**Electropedia - www.electropedia.org**
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 62056-5-3

Edition 4.0 2023-09

# 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 978-2-8322-7223-7

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

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

# CONTENTS

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

5.3.1 Overview ..... 72
5.3.2 Hash function ..... 72
5.3.3 Symmetric key algorithms ..... 73
5.3.4 Public key algorithms ..... 80
5.3.5 Random number generation ..... 90
5.3.6 Compression ..... 91
5.3.7 Security suite ..... 91
5.4 Cryptographic keys – overview ..... 92
5.5 Key used with symmetric key algorithms ..... 92
5.5.1 Symmetric keys types ..... 92
5.5.2 Key information with general-ciphering APDU and data protection ..... 94
5.5.3 Key identification ..... 94
5.5.4 Key wrapping ..... 95
5.5.5 Key agreement ..... 95
5.5.6 Symmetric key cryptoperiods ..... 96
5.6 Keys used with public key algorithms ..... 96
5.6.1 Overview ..... 96
5.6.2 Key pair generation ..... 96
5.6.3 Public key certificates and infrastructure ..... 97
5.6.4 Certificate and certificate extension profile ..... 100
5.6.5 Suite B end entity certificate types to be supported by DLMS®/COSEM servers ..... 108
5.6.6 Management of certificates ..... 108
5.7 Applying cryptographic protection ..... 113
5.7.1 Overview ..... 113
5.7.2 Protecting xDLMS APDUs ..... 113
5.7.3 Multi-layer protection by multiple parties ..... 126
5.7.4 HLS authentication mechanisms ..... 127
5.7.5 Protecting COSEM data ..... 130
6 DLMS®/COSEM application layer service specification ..... 131
6.1 Service primitives and parameters ..... 131
6.2 The COSEM-OPEN service ..... 133
6.3 The COSEM-RELEASE service ..... 138
6.4 COSEM-ABORT service ..... 141
6.5 Protection and general block transfer parameters ..... 141
6.6 The GET service ..... 146
6.7 The SET service ..... 149
6.8 The ACTION service ..... 153
6.9 The ACCESS service ..... 156
6.9.1 Overview – Main features ..... 156
6.9.2 Service specification ..... 158
6.10 The DataNotification service ..... 162
6.11 The EventNotification service ..... 164
6.12 The TriggerEventNotificationSending service ..... 165
6.13 Variable access specification ..... 166
6.14 The Read service ..... 166
6.15 The Write service ..... 170
6.16 The UnconfirmedWrite service ..... 173
6.17 The InformationReport service ..... 175

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

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

H.3 Example of an end entity digital signature Certificate using P-256 signed with P-256 ..... 356
Annex I (normative) Use of key agreement schemes in DLMS®/COSEM ..... 357
I.1 Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme ..... 357
I.2 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme ..... 360
I.3 Static Unified Model C(0e, 2s, ECC CDH) scheme ..... 363
Annex J (informative) Exchanging protected xDLMS APDUs between TP and server ..... 367
J.1 General ..... 367
J.2 Example 1: Protection is the same in the two directions ..... 367
J.3 Example 2: Protection is different in the two directions ..... 368
Annex K (informative) Significant technical changes with respect to IEC 62056-5-3:2017 ..... 370
Bibliography ..... 373

Figure 1 – Client–server model and communication protocols ..... 41
Figure 2 – Naming and addressing in DLMS®/COSEM ..... 42
Figure 3 – A complete communication session in the CO environment ..... 44
Figure 4 – DLMS®/COSEM messaging patterns ..... 47
Figure 5 – DLMS®/COSEM generic communication profile ..... 49
Figure 6 – Model of a DLMS®/COSEM metering system ..... 50
Figure 7 – DLMS®/COSEM server model ..... 51
Figure 8 – Model of a DLMS®/COSEM client using multiple protocol stacks ..... 52
Figure 9 – The structure of the DLMS®/COSEM application layers ..... 54
Figure 10 – The concept of composable xDLMS messages ..... 61
Figure 11 – Summary of DLMS®/COSEM AL services ..... 64
Figure 12 – Authentication mechanisms ..... 67
Figure 13 – Client – server message security concept ..... 70
Figure 14 – End-to-end message security concept ..... 71
Figure 15 – Hash function ..... 73
Figure 16 – Encryption and decryption ..... 74
Figure 17 – Message Authentication Codes (MACs) ..... 75
Figure 18 – GCM functions ..... 77
Figure 19 – Digital signatures ..... 83
Figure 20 – C(2e, 0s) scheme: each party contributes only an ephemeral key pair ..... 85
Figure 21 – C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair ..... 86
Figure 22 – C(0e, 2s) scheme: each party contributes only a static key pair ..... 88
Figure 23 – Architecture of a Public Key Infrastructure (example) ..... 99
Figure 24 – MSC for provisioning the server with CA certificates ..... 109
Figure 25 – MSC for security personalisation of the server ..... 110
Figure 26 – Provisioning the server with the certificate of the client ..... 111
Figure 27 – Provisioning the client / third party with a certificate of the server ..... 112
Figure 28 – Remove certificate from the server ..... 112
Figure 29 – Cryptographic protection of information using AES-GCM ..... 116
Figure 30 – Structure of service-specific global / dedicated ciphering xDLMS APDUs ..... 118

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

Figure 70 – GET service with partial invocations, GBT and streaming, recovery of last block ..... 239
Figure 71 – SET service with GBT, with server not supporting streaming, recovery of 3rd block ..... 240
Figure 72 – ACTION-WITH-LIST service with bi-directional GBT and block recovery ..... 241
Figure 73 – DataNotification service with GBT with partial invocation ..... 243
Figure B.1 – Short wrapper ..... 287
Figure C.1 – General architecture with gateway ..... 288
Figure C.2 – The fields used for pre-fixing the COSEM APDUs ..... 289
Figure C.3 – Pull message sequence chart ..... 290
Figure C.4 – Push message sequence chart ..... 291
Figure I.1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme ..... 357
Figure I.2 – Ciphered xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme ..... 360
Figure I.3 – Ciphered xDLMS APDU protected by an ephemeral key established using the Static Unified Model C(0e, 2s, ECC CDH) scheme ..... 364
Figure J.1 – Exchanging protected xDLMS APDUs between TP and server: example 1 ..... 368
Figure J.2 – Exchanging protected xDLMS APDUs between TP and server: example 2 ..... 369

Table 1 – Client and server SAPs ..... 43
Table 2 – Clarification of the meaning of PDU size for DLMS®/COSEM ..... 63
Table 3 – Elliptic curves in DLMS®/COSEM security suites ..... 81
Table 4 – Ephemeral Unified Model key agreement scheme summary ..... 85
Table 5 – One-pass Diffie-Hellman key agreement scheme summary ..... 87
Table 6 – Static Unified Model key agreement scheme summary ..... 89
Table 7 – *OtherInfo* subfields and substrings ..... 90
Table 8 – Security algorithm ID-s ..... 90
Table 9 – DLMS®/COSEM security suites ..... 91
Table 10 – Symmetric keys types ..... 93
Table 11 – Key information with general-ciphering APDU and data protection ..... 94
Table 12 – Asymmetric keys types and their use ..... 96
Table 13 – X.509 v3 Certificate structure ..... 100
Table 14 – X.509 v3 tbsCertificate fields ..... 101
Table 15 – Naming scheme for the Root-CA instance (informative) ..... 102
Table 16 – Naming scheme for the Sub-CA instance (informative) ..... 102
Table 17 – Naming scheme for the end entity instance ..... 103
Table 18 – X.509 v3 Certificate extensions ..... 105
Table 19 – Key Usage extensions ..... 106
Table 20 – Subject Alternative Name values ..... 106
Table 21 – Issuer Alternative Name values ..... 107
Table 22 – Basic constraints extension values ..... 107
Table 23 – Certificates handled by DLMS®/COSEM end entities ..... 108
Table 24 – Security policy values ("Security setup" version 1) ..... 113

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

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

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