



INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 17.220, 35.110, 91.140.50

ISBN 978-2-8322-7223-7

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

CONTENTS

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

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

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

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

H.3	Example of an end entity digital signature Certificate using P-256 signed with P-256	356
Annex I (normative)	Use of key agreement schemes in DLMS®/COSEM.....	357
I.1	Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	357
I.2	One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme	360
I.3	Static Unified Model C(0e, 2s, ECC CDH) scheme	363
Annex J (informative)	Exchanging protected xDLMS APDUs between TP and server	367
J.1	General.....	367
J.2	Example 1: Protection is the same in the two directions	367
J.3	Example 2: Protection is different in the two directions	368
Annex K (informative)	Significant technical changes with respect to IEC 62056-5-3:2017.....	370
Bibliography	373
Figure 1	– Client–server model and communication protocols	41
Figure 2	– Naming and addressing in DLMS®/COSEM	42
Figure 3	– A complete communication session in the CO environment.....	44
Figure 4	– DLMS®/COSEM messaging patterns	47
Figure 5	– DLMS®/COSEM generic communication profile	49
Figure 6	– Model of a DLMS®/COSEM metering system	50
Figure 7	– DLMS®/COSEM server model.....	51
Figure 8	– Model of a DLMS®/COSEM client using multiple protocol stacks.....	52
Figure 9	– The structure of the DLMS®/COSEM application layers	54
Figure 10	– The concept of composable xDLMS messages.....	61
Figure 11	– Summary of DLMS®/COSEM AL services	64
Figure 12	– Authentication mechanisms.....	67
Figure 13	– Client – server message security concept	70
Figure 14	– End-to-end message security concept.....	71
Figure 15	– Hash function.....	73
Figure 16	– Encryption and decryption	74
Figure 17	– Message Authentication Codes (MACs).....	75
Figure 18	– GCM functions	77
Figure 19	– Digital signatures	83
Figure 20	– C(2e, 0s) scheme: each party contributes only an ephemeral key pair.....	85
Figure 21	– C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair	86
Figure 22	– C(0e, 2s) scheme: each party contributes only a static key pair.....	88
Figure 23	– Architecture of a Public Key Infrastructure (example)	99
Figure 24	– MSC for provisioning the server with CA certificates	109
Figure 25	– MSC for security personalisation of the server	110
Figure 26	– Provisioning the server with the certificate of the client	111
Figure 27	– Provisioning the client / third party with a certificate of the server.....	112
Figure 28	– Remove certificate from the server.....	112
Figure 29	– Cryptographic protection of information using AES-GCM.....	116
Figure 30	– Structure of service-specific global / dedicated ciphering xDLMS APDUs	118

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

Figure 70 – GET service with partial invocations, GBT and streaming, recovery of last block.....	239
Figure 71 – SET service with GBT, with server not supporting streaming, recovery of 3 rd block.....	240
Figure 72 – ACTION-WITH-LIST service with bi-directional GBT and block recovery	241
Figure 73 – DataNotification service with GBT with partial invocation.....	243
Figure B.1 – Short wrapper	287
Figure C.1 – General architecture with gateway	288
Figure C.2 – The fields used for pre-fixing the COSEM APDUs	289
Figure C.3 – Pull message sequence chart	290
Figure C.4 – Push message sequence chart	291
Figure I.1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme	357
Figure I.2 – Ciphred xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme.....	360
Figure I.3 – Ciphred xDLMS APDU protected by an ephemeral key established using the Static Unified Model C(0e, 2s, ECC CDH) scheme	364
Figure J.1 – Exchanging protected xDLMS APDUs between TP and server: example 1.....	368
Figure J.2 – Exchanging protected xDLMS APDUs between TP and server: example 2.....	369
Table 1 – Client and server SAPs	43
Table 2 – Clarification of the meaning of PDU size for DLMS®/COSEM	63
Table 3 – Elliptic curves in DLMS®/COSEM security suites	81
Table 4 – Ephemeral Unified Model key agreement scheme summary	85
Table 5 – One-pass Diffie-Hellman key agreement scheme summary	87
Table 6 – Static Unified Model key agreement scheme summary	89
Table 7 – <i>OtherInfo</i> subfields and substrings	90
Table 8 – Security algorithm ID-s	90
Table 9 – DLMS®/COSEM security suites.....	91
Table 10 – Symmetric keys types.....	93
Table 11 – Key information with general-ciphering APDU and data protection.....	94
Table 12 – Asymmetric keys types and their use.....	96
Table 13 – X.509 v3 Certificate structure	100
Table 14 – X.509 v3 tbsCertificate fields	101
Table 15 – Naming scheme for the Root-CA instance (informative).....	102
Table 16 – Naming scheme for the Sub-CA instance (informative).....	102
Table 17 – Naming scheme for the end entity instance	103
Table 18 – X.509 v3 Certificate extensions	105
Table 19 – Key Usage extensions	106
Table 20 – Subject Alternative Name values	106
Table 21 – Issuer Alternative Name values	107
Table 22 – Basic constraints extension values	107
Table 23 – Certificates handled by DLMS®/COSEM end entities.....	108
Table 24 – Security policy values ("Security setup" version 1)	113

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

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ELECTRICITY METERING DATA EXCHANGE – THE DLMS®/COSEM SUITE –

Part 5-3: DLMS®/COSEM application layer

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This fourth edition cancels and replaces the third edition published in 2017. This edition constitutes a technical revision.

The significant technical changes with respect to the previous edition are listed in Annex K (Informative).

The text of this International Standard is based on the following documents:

Draft	Report on voting
13/1890/FDIS	13/1904/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all the parts in the IEC 62056 series, published under the general title *Electricity metering data exchange – The DLMS®/COSEM suite*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This fourth edition of IEC 62056-5-3 has been prepared by IEC TC13 WG14 with a significant contribution of the DLMS® User Association, its A-type liaison partner.

This edition is in line with DLMS® UA 1000-2, the "Green Book" Ed. 10:2020 and DLMS® UA 1000-2, the "Green Book" Ed. 10 Amendment 1 2021.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning the stack of protocols on which the present standard IEC 62056-5-3 is based.

The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the IEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions for applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the IEC. Information may be obtained from:

DLMS¹ User Association
www.dlms.com

¹ Device Language Message Specification.

ELECTRICITY METERING DATA EXCHANGE – THE DLMS®/COSEM SUITE –

Part 5-3: DLMS®/COSEM application layer

1 Scope

This part of IEC 62056 specifies the DLMS®/COSEM application layer in terms of structure, services and protocols for DLMS®/COSEM clients and servers, and defines rules to specify the DLMS®/COSEM communication profiles.

It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2:2021 using either logical name (LN) or short name (SN) referencing.

Annex A (normative) defines how to use the COSEM application layer in various communication profiles. It specifies how various communication profiles can be constructed for exchanging data with metering equipment using the COSEM interface model, and what are the necessary elements to specify in each communication profile. The actual, media-specific communication profiles are specified in separate parts of the IEC 62056 series.

Annex B (normative) specifies the SMS short wrapper.

Annex C (normative) specifies the gateway protocol.

Annex D, Annex E and Annex F (informative) include encoding examples for APDUs.

Annex G (normative) provides NSA Suite B elliptic curves and domain parameters.

Annex H (informative) provides an example of an End entity signature certificate using P-256 signed with P-256.

Annex I (normative) specifies the use of key agreement schemes in DLMS®/COSEM.

Annex J (informative) provides examples of exchanging protected xDLMS APDUs between a third party and a server.

Annex K (informative) lists the main technical changes in this fourth edition.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61334-4-41:1996, *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocols – Distribution line message specification*

IEC 61334-6:2000, *Distribution automation using distribution line carrier systems – Part 6: A-XDR encoding rule*

IEC TR 62051:1999, *Electricity metering – Glossary of terms*

IEC TR 62051-1:2004, *Electricity metering – Data exchange for meter reading, tariff and load control – Glossary of terms – Part 1: Terms related to data exchange with metering equipment using DLMS®/COSEM*

IEC 62056-6-2:2021, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 6-2: COSEM interface classes*

IEC 62056-7-3:2017, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 7-3: Wired and wireless M-Bus communication profiles for local and neighbourhood networks*

IEC 62056-7-6:2013, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 7-6: The 3-layer, connection-oriented HDLC based communication profile*

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

IEC 62056-8-11:–² *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-11: Communication profile for Wi-SUN field area mesh networks*

IEC 62056-8-12:–³ *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-12: Communication profile for Low Power Wide Area Networks (LPWAN)*

IEC 62056-9-7:2013, *Electricity metering data exchange – The DLMS®/COSEM suite – Part 9-7: Communication profile for TCP-UDP/IP networks*

ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1) – Part 1: Specification of basic notation*

ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules – Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 15953:1999, *Information technology – Open Systems Interconnection – Service definition for the Application Service Object Association Control Service Element*

NOTE This standard cancels and replaces ISO/IEC 8649:1996 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.

ISO/IEC 15954:1999, *Information technology – Open Systems Interconnection – Connection-mode protocol for the Application Service Object Association Control Service Element*

NOTE This standard cancels and replaces ISO/IEC 8650-1:1999 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.

ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ITU-T X.509:2008, *SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY – Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

² Under preparation. Stage at the time of publication: IEC CDV.

³ Under preparation. Stage at the time of publication: 13/1877/CDV:2023.

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

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

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

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

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

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

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

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

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

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

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

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

SEC1:2009, *Standards for Efficient Cryptography: Elliptic Curve Cryptography*. SECG. Version 2.0

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002 <http://tools.ietf.org/html/rfc3394>

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)* <http://www.rfc-editor.org/rfc/rfc4106.txt>

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

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

SOMMAIRE

AVANT-PROPOS	386
INTRODUCTION	388
1 Domaine d'application	389
2 Références normatives	390
3 Termes, définitions, abréviations et symboles	392
3.1 Définitions générales concernant DLMS®/COSEM	392
3.2 Définitions liées à la sécurité cryptée	396
3.3 Définitions et abréviations liées au mode Galois/Counter	407
3.4 Abréviations générales	409
3.5 Symboles liés au mode Galois/Counter	413
3.6 Symboles liés à l'algorithme ECDSA	413
3.7 Symboles liés aux algorithmes à agrément de clé	414
4 Vue d'ensemble de DLMS®/COSEM	414
4.1 Échange d'informations dans DLMS®/COSEM	414
4.1.1 Généralités	414
4.1.2 Modèle de communication	415
4.1.3 Nommage et adressage	416
4.1.4 Opération orientée connexion	419
4.1.5 Associations d'applications	420
4.1.6 Type de messagerie	422
4.1.7 Échange de données entre des tierces parties et des serveurs DLMS®/COSEM	423
4.1.8 Profils de communication	423
4.1.9 Modèle de système de comptage DLMS®/COSEM	424
4.1.10 Modèle de serveurs DLMS®/COSEM	425
4.1.11 Modèle d'un client DLMS®/COSEM	427
4.1.12 Interopérabilité et interconnectivité dans DLMS®/COSEM	428
4.1.13 Assurance d'interconnectivité: service d'identification de protocole	428
4.1.14 Intégration de système et installation de comptage	428
4.2 Principales caractéristiques de la couche application DLMS®/COSEM	429
4.2.1 Généralités	429
4.2.2 Structure de la couche application DLMS®/COSEM	429
4.2.3 Élément de service de contrôle d'association (ACSE)	431
4.2.4 Élément de service d'application xDLMS	432
4.2.5 Services de gestion de couche	440
4.2.6 Récapitulatif des services de la couche application DLMS®/COSEM	440
4.2.7 Protocoles de la couche application DLMS®/COSEM	441
5 Sécurité des informations dans DLMS®/COSEM	442
5.1 Vue d'ensemble	442
5.2 Concept de sécurité DLMS®/COSEM	442
5.2.1 Vue d'ensemble	442
5.2.2 Identification et authentification	442
5.2.3 Contexte de sécurité	446
5.2.4 Droits d'accès	446
5.2.5 Sécurité des messages de la couche application	447
5.2.6 Sécurité des données COSEM	449
5.3 Algorithmes cryptographiques	449

5.3.1	Vue d'ensemble	449
5.3.2	Fonction de hachage	450
5.3.3	Algorithmes à clé symétrique	451
5.3.4	Algorithmes à clé publique	458
5.3.5	Génération de nombres aléatoires	470
5.3.6	Compression	470
5.3.7	Suite de sécurité	470
5.4	Clés cryptographiques — Vue d'ensemble	471
5.5	Clés utilisées avec des algorithmes à clé symétrique	471
5.5.1	Types de clés symétriques	471
5.5.2	Informations relatives aux clés avec APDU general-ciphering et protection des données	474
5.5.3	Identification de clé	475
5.5.4	Enveloppement de clé	475
5.5.5	Agrément de clé	475
5.5.6	Périodes cryptographiques à clé symétrique	476
5.6	Clés utilisées avec des algorithmes à clé publique	476
5.6.1	Vue d'ensemble	476
5.6.2	Génération de paires de clés	477
5.6.3	Certificats de clé publique et infrastructure à clé publique	477
5.6.4	Certificat et profil d'extension de certificat	480
5.6.5	Types de certificats d'entités finales de la Suite B à prendre en charge par les serveurs DLMS@/COSEM	488
5.6.6	Gestion des certificats	489
5.7	Application de la protection cryptographique	494
5.7.1	Vue d'ensemble	494
5.7.2	Protection des APDU xDLMS	494
5.7.3	Protection multicouche par plusieurs parties	507
5.7.4	Mécanismes d'authentification HLS	508
5.7.5	Protection des données COSEM	511
6	Spécification de service de la couche application DLMS@/COSEM	512
6.1	Primitives de service et paramètres	512
6.2	Service COSEM-OPEN	514
6.3	Service COSEM-RELEASE	519
6.4	Service COSEM-ABORT	522
6.5	Paramètres de protection et de transfert de bloc général	523
6.6	Service GET	529
6.7	Service SET	532
6.8	Service ACTION	537
6.9	Service ACCESS	541
6.9.1	Vue d'ensemble — Principales fonctionnalités	541
6.9.2	Spécification de service	543
6.10	Service DataNotification	548
6.11	Service EventNotification	549
6.12	Service TriggerEventNotificationSending	551
6.13	Spécification d'accès variable	551
6.14	Service Read	552
6.15	Service Write	556
6.16	Service UnconfirmedWrite	560

6.17	Service InformationReport	561
6.18	Services de gestion de couches côté client: Service SetMapperTable.request.....	562
6.19	Récapitulatif des services et de la mise en correspondance de services de transfert de données LN/SN	562
7	Spécification du protocole de couche application DLMS@/COSEM	564
7.1	Fonction de commande	564
7.1.1	Définitions des états de la fonction de commande côté client.....	564
7.1.2	Définitions des états de la fonction de commande côté serveur	565
7.2	Services ACSE et APDU	567
7.2.1	Unités fonctionnelles ACSE, services et paramètres de service	567
7.2.2	Noms COSEM enregistrés	570
7.2.3	Règles de codage d'APDU.....	573
7.2.4	Protocole d'établissement d'association d'applications	573
7.2.5	Protocole de libération d'association d'applications	579
7.3	Protocole des services de transfert de données	582
7.3.1	Négociation de services et d'options — Bloc de conformité	582
7.3.2	Appels de service confirmés et non confirmés	583
7.3.3	Protocole du service GET	585
7.3.4	Protocole du service SET	588
7.3.5	Protocole du service ACTION	591
7.3.6	Protocole du service ACCESS	593
7.3.7	Protocole du service DataNotification	595
7.3.8	Protocole du service EventNotification.....	598
7.3.9	Protocole du service Read.....	599
7.3.10	Protocole du service Write.....	603
7.3.11	Protocole du service UnconfirmedWrite	607
7.3.12	Protocole du service InformationReport	608
7.3.13	Protocole du mécanisme de transfert de bloc général.....	609
7.3.14	Protocole de mécanisme d'exception.....	632
8	Syntaxe abstraite des APDU ACSE et COSEM	633
9	Schéma XML des APDU COSEM.....	652
9.1	Généralités	652
9.2	Schéma XML	652
Annexe A (normative) Utilisation de la couche application DLMS@/COSEM dans différents profils de communication		
A.1	Généralités	674
A.2	Environnements de communication ciblés.....	674
A.3	Structure du profil	674
A.4	Schémas d'identification et d'adressage	674
A.5	Services de couche de support et mise en correspondance de services.....	675
A.6	Paramètres spécifiques au profil de communication des services d'AL COSEM.....	675
A.7	Considérations / contraintes spécifiques à l'utilisation de certains services dans un profil donné	675
A.8	Profil de communication à 3 couches, orienté connexion et basé sur HDLC	675
A.9	Profils de communication basés sur TCP-UDP/IP (COSEM_on_IP).....	675
A.10	Profils de communication M-Bus filaire et sans fil.....	675
A.11	Profil PLC S-FSK	675

Annexe G (normative) Courbes elliptiques et paramètres de domaine de la Suite B NSA.....	742
Annexe H (informative) Exemple de certificat de signature d'entité finale utilisant P-256 signé avec P-256.....	744
H.1 Champs des certificats de clé publique	744
H.2 Exemple de certificat Root-CA utilisant P-256 signé avec P-256	745
H.3 Exemple de certificat de signature numérique d'entité finale utilisant P-256 signé avec P-256	746
Annexe I (normative) Utilisation des mécanismes d'agrément de clé dans DLMS®/COSEM.....	747
I.1 Schéma Ephemeral Unified Model C(2e, 0s, ECC CDH).....	747
I.2 Schéma One-pass Diffie-Hellman C(1e, 1s, ECC CDH).....	750
I.3 Schéma de modèle unifié statique C(0e, 2s, ECC CDH).....	753
Annexe J (informative) Échange d'APDU xDLMS protégées entre TP et serveur.....	757
J.1 Généralités	757
J.2 Exemple 1: protection similaire dans les deux sens.....	757
J.3 Exemple 2: protection différente dans les deux sens.....	758
Annexe K (informative) Modifications techniques majeures par rapport à l'IEC 62056-5-3:2017	760
Bibliographie.....	763
Figure 1 – Modèle client/serveur et protocoles de communication.....	416
Figure 2 – Nommage et adressage dans DLMS®/COSEM	417
Figure 3 – Session complète de communication dans l'environnement CO.....	420
Figure 4 – Types de messagerie DLMS®/COSEM.....	422
Figure 5 – Profil générique de communication DLMS®/COSEM	424
Figure 6 – Modèle de système de comptage DLMS®/COSEM.....	425
Figure 7 – Modèle de serveur DLMS®/COSEM	426
Figure 8 – Modèle de client DLMS®/COSEM utilisant plusieurs piles de protocoles	427
Figure 9 – Structure des couches d'application DLMS®/COSEM.....	430
Figure 10 – Concept de messages xDLMS composables	438
Figure 11 – Récapitulatif des services de l'AL DLMS®/COSEM	441
Figure 12 – Mécanismes d'authentification.....	444
Figure 13 – Conception de sécurité des messages client-serveur	447
Figure 14 – Concept de sécurité de bout en bout sur les messages	448
Figure 15 – Fonction de hachage.....	450
Figure 16 – Cryptage et décryptage	451
Figure 17 – Codes d'authentification de message (MAC)	453
Figure 18 – Fonctions du GCM	454
Figure 19 – Signatures numériques.....	461
Figure 20 – Schéma C(2e, 0s): chaque partie apporte uniquement une paire de clés éphémères.....	463
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	465
Figure 22 – Schéma C(0e, 2s): chaque partie apporte uniquement une paire de clés statiques	467
Figure 23 – Architecture d'une infrastructure à clé publique (exemple).....	479

Figure 24 – MSC pour l’approvisionnement du serveur en certificats de la CA	490
Figure 25 – MSC pour la personnalisation de sécurité du serveur	491
Figure 26 – Approvisionnement du serveur en certificat du client	492
Figure 27 – Approvisionnement du client/de la tierce partie en certificat du serveur	493
Figure 28 – Suppression de certificat du serveur	493
Figure 29 – Protection cryptographique des informations à l’aide d’AES-GCM	497
Figure 30 – Structure des APDU xDLMS de chiffrement global spécifique au service / de chiffrement dédié spécifique au service.....	499
Figure 31 – Structure des APDU xDLMS general-glo-ciphering et general-ded- ciphering.....	500
Figure 32 – Structure des APDU xDLMS general-ciphering.....	501
Figure 33 – Structure des APDU general-signing	507
Figure 34 – Primitives de service	512
Figure 35 – Diagrammes de séquences temporelles	513
Figure 36 – Paramètres de service supplémentaires pour contrôler la protection cryptographique et le GBT	524
Figure 37 – Diagramme d’états partiel pour la fonction de commande côté client.....	564
Figure 38 – Diagramme d’états partiel pour la fonction de commande côté serveur.....	566
Figure 39 – MSC pour l’établissement réussi d’une AA précédé de l’établissement réussi d’une connexion de couches inférieures	575
Figure 40 – Libération d’AA sans perte de données à l’aide du service A-RELEASE	580
Figure 41 – Libération d’AA sans perte de données par déconnexion de la couche de support	581
Figure 42 – Abandon d’une AA après la primitive PH-ABORT.indication	582
Figure 43 – MSC du service GET	586
Figure 44 – MSC du service GET avec transfert de blocs.....	586
Figure 45 – MSC du service GET avec transfert de blocs, transfert long abandonné.....	588
Figure 46 – MSC du service SET	589
Figure 47 – MSC du service SET avec transfert de blocs	590
Figure 48 – MSC du service ACTION	592
Figure 49 – MSC du service ACTION avec transfert de bloc	593
Figure 50 – Service ACCESS avec réponse longue	594
Figure 51 – Service ACCESS avec demande et réponse longues	595
Figure 52 – MSC pour le service DataNotification, situation 1)	596
Figure 53 – MSC pour le service DataNotification, situation 2)	597
Figure 54 – MSC pour le service DataNotification, situation 3)	598
Figure 55 – MSC du service Read utilisé pour lire un attribut	601
Figure 56 – MSC du service Read utilisé pour appeler une méthode.....	601
Figure 57 – MSC du service Read utilisé pour lire un attribut, avec transfert de blocs.....	602
Figure 58 – MSC du service Write utilisé pour écrire un attribut	606
Figure 59 – MSC du service Write utilisé pour appeler une méthode.....	606
Figure 60 – MSC du service Write utilisé pour écrire un attribut, avec transfert de blocs.....	607
Figure 61 – MSC du service UnconfirmedWrite utilisé pour écrire un attribut	608
Figure 62 – Appels de service partiels et APDU GBT	611
Figure 63 – Procédure de GBT	614

Figure 64 – Sous-procédure Envoyer le flux d’APDU GBT	618
Figure 65 – Sous-procédure Traiter l’APDU GBT	620
Figure 66 – Sous-procédure Vérifier la RQ et combler les trous	622
Figure 67 – Service GET avec GBT, passage à la diffusion en flux	623
Figure 68 – Service GET avec appels partiels, GBT et en flux, récupération du 4 ^e bloc envoyé dans le 2 ^e flux	625
Figure 69 – Service GET avec appels partiels, GBT et en flux, récupération des 4 ^e et 5 ^e blocs	626
Figure 70 – Service GET avec appels partiels, GBT et en flux, récupération du dernier bloc.....	627
Figure 71 – Service SET avec GBT, avec serveur ne prenant pas en charge du flux, récupération du 3 ^e bloc	628
Figure 72 – Service ACTION-WITH-LIST avec GBT bidirectionnel et récupération de blocs.....	629
Figure 73 – Service DataNotification avec GBT, avec appel partiel	631
Figure B.1 – Couche d’adaptation réduite	676
Figure C.1 – Architecture générale avec passerelle	677
Figure C.2 – Champs utilisés pour le préfixage des APDU COSEM.....	678
Figure C.3 – Tableau de séquence de messages Pull	679
Figure C.4 – Tableau de séquence de messages Push	680
Figure I.1 – MSC pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH)	747
Figure I.2 – APDU xDLMS chiffrée protégée par une clé éphémère établie à l’aide d’un schéma One-pass Diffie-Hellman (1e, 1s, ECC CDH)	750
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)	754
Figure J.1 – Échange d’APDU xDLMS protégées entre TP et serveur: exemple 1	758
Figure J.2 – Échange d’APDU xDLMS protégées entre TP et serveur: exemple 2	759
Tableau 1 – SAP client et serveur	418
Tableau 2 —Explication de la signification des paramètres PDU Size pour DLMS®/COSEM.....	440
Tableau 3 – Courbes elliptiques dans les suites de sécurité DLMS®/COSEM	459
Tableau 4 – Récapitulatif de mécanisme d’agrément de clé Ephemeral Unified Model	464
Tableau 5 – Récapitulatif de mécanisme d’agrément de clé One-pass Diffie-Hellman	466
Tableau 6 – Récapitulatif du mécanisme d’agrément de clé du modèle unifié statique	468
Tableau 7 – Sous-champs et sous-chaînes <i>OtherInfo</i>	469
Tableau 8 – ID d’algorithmes de sécurité	470
Tableau 9 – Suites de sécurité DLMS®/COSEM	471
Tableau 10 – Types de clés symétriques	473
Tableau 11 – Informations relatives aux clés avec APDU general-ciphering et protection des données.....	474
Tableau 12 – Types de clés asymétriques et leur utilisation	476
Tableau 13 – Structure de certificat X.509 v3.....	481
Tableau 14 – Champs du tbsCertificate X.509 v3.....	482

Tableau 15 – Schéma de nommage pour l'instance de la Root-CA (informatif).....	483
Tableau 16 – Schéma de nommage pour l'instance de la Sub-CA (informatif).....	483
Tableau 17 – Schéma de nommage pour l'instance de l'entité finale.....	483
Tableau 18 – Extensions de certificat X.509 v3.....	485
Tableau 19 – Extensions KeyUsage.....	486
Tableau 20 – Valeurs Subject Alternative Name (nom alternatif d'objet).....	487
Tableau 21 – Valeurs Issuer Alternative Name (nom alternatif de l'émetteur).....	487
Tableau 22 – Valeurs de l'extension Basic Constraints.....	488
Tableau 23 – Certificats traités par des entités finales DLMS®/COSEM.....	489
Tableau 24 – Valeurs de la politique de sécurité ("Security setup" version 1).....	494
Tableau 25 – Valeurs des droits d'accès ("Association LN" ver 3, "Association SN" ver 4).....	495
Tableau 26 – APDU xDLMS chiffrées.....	496
Tableau 27 – Octet de contrôle de sécurité.....	498
Tableau 28 – Texte brut et données supplémentaires authentifiées.....	498
Tableau 29 – Utilisation des champs des APDU xDLMS de chiffrement.....	502
Tableau 30 – Exemple: APDU xDLMS glo-get-request.....	503
Tableau 31 – Service ACCESS avec le mécanisme d'agrément de clé One-pass Diffie-Hellman C(1e, 1s, ECC CDH) et general-ciphering.....	505
Tableau 32 – Mécanismes d'authentification HLS DLMS®/COSEM.....	509
Tableau 33 – Exemple de HLS utilisant le mécanisme d'authentification 5 avec GMAC.....	510
Tableau 34 – Exemple de HLS utilisant le mécanisme d'authentification 7 avec ECDSA.....	511
Tableau 35 – Codes des paramètres de service de l'AL.....	514
Tableau 36 – Paramètres de service des primitives de service COSEM-OPEN.....	515
Tableau 37 – Paramètres de service des primitives de service COSEM-RELEASE.....	520
Tableau 38 – Paramètres de service des primitives de service COSEM-ABORT.....	523
Tableau 39 – Paramètres de service supplémentaires.....	525
Tableau 40 – Paramètres de sécurité.....	526
Tableau 41 – APDU utilisées avec les types de protections de sécurité (Security_Protection_Type).....	528
Tableau 42 – Paramètres de service du service GET.....	530
Tableau 43 – Types de demandes et de réponses du service GET.....	531
Tableau 44 – Paramètres de service du service SET.....	533
Tableau 45 – Types de demandes et de réponses du service SET.....	534
Tableau 46 – Paramètres de service du service ACTION.....	537
Tableau 47 – Types de demandes et de réponses du service ACTION.....	538
Tableau 48 – Paramètres de service du service ACCESS.....	545
Tableau 49 – Paramètres de service des primitives de service DataNotification.....	548
Tableau 50 – Paramètres de service des primitives de service EventNotification.....	550
Tableau 51 – Paramètres de service de la primitive de service TriggerEventNotificationSending.request.....	551
Tableau 52 – Spécification d'accès variable.....	551
Tableau 53 – Paramètres de service du service Read.....	552
Tableau 54 – Utilisation des variantes du paramètre Variable_Access_Specification et des choix pour Read.response.....	554

Tableau 55 – Paramètres de service du service Write.....	557
Tableau 56 – Utilisation des variantes de Variable_Access_Specification et des choix pour Write.response.....	558
Tableau 57 – Paramètres de service du service UnconfirmedWrite	560
Tableau 58 – Utilisation des variantes de Variable_Access_Specification	560
Tableau 59 – Paramètres de service du service InformationReport	562
Tableau 60 – Paramètres de service des primitives de service SetMapperTable.request	562
Tableau 61 – Récapitulatif des services ACSE.....	563
Tableau 62 – Récapitulatif des services xDLMS.....	563
Tableau 63 – APDU d'unité fonctionnelle et leurs champs.....	568
Tableau 64 – Noms de contexte d'application COSEM.....	572
Tableau 65 – Noms de mécanismes d'authentification COSEM.....	572
Tableau 66 – ID d'algorithmes cryptographiques.....	573
Tableau 67 – Bloc de conformité xDLMS.....	583
Tableau 68 – Types de service GET et APDU	585
Tableau 69 – Types de service SET et APDU	589
Tableau 70 – Types de service ACTION et APDU	592
Tableau 71 – Mise en correspondance du service GET et du service Read.....	599
Tableau 72 – Mise en correspondance du service ACTION et du service Read.....	600
Tableau 73 – Mise en correspondance du service SET et du service Write	603
Tableau 74 – Mise en correspondance du service ACTION et du service Write.....	604
Tableau 75 – Mise en correspondance du service SET et du service UnconfirmedWrite.....	608
Tableau 76 – Mise en correspondance du service ACTION et du service UnconfirmedWrite	608
Tableau 77 – Mise en correspondance des services EventNotification et InformationReport	609
Tableau 78 – Variables d'états de la procédure de GBT.....	616
Tableau 79 – Mécanisme d'exception xDLMS	632
Tableau B.1 – Processus d'application réservés	676
Tableau D.1 – Bloc de conformité	683
Tableau D.2 – Codage A-XDR de l'APDU xDLMS InitiateRequest	684
Tableau D.3 – Codage A-XDR de l'APDU xDLMS InitiateResponse	685
Tableau D.4 – Codage BER de l'APDU AARQ	688
Tableau D.5 – APDU AARQ complète	690
Tableau D.6 – Codage BER de l'APDU AARE.....	691
Tableau D.7 – APDU AARE complète	695
Tableau E.1 – Codage A-XDR de l'APDU xDLMS InitiateRequest	697
Tableau E.2 – Cryptage authentifié de l'APDU xDLMS InitiateRequest	698
Tableau E.3 – Codage BER de l'APDU AARQ.....	699
Tableau E.4 – Codage A-XDR de l'APDU xDLMS InitiateResponse	701
Tableau E.5 – Cryptage authentifié de l'APDU xDLMS InitiateResponse.....	702
Tableau E.6 – Codage BER de l'APDU AARE	703
Tableau E.7 – Codage BER de l'APDU RLRQ.....	704
Tableau E.8 – Codage BER de l'APDU RLRE	705

Tableau F.1 – Objets utilisés dans les exemples	706
Tableau F.2 – Exemple: lecture de la valeur d'un attribut unique sans transfert de blocs	707
Tableau F.3 – Exemple: lecture de la valeur d'une liste d'attributs sans transfert de blocs	708
Tableau F.4 – Exemple: lecture de la valeur d'un attribut unique avec transfert de blocs	710
Tableau F.5 – Exemple: lecture de la valeur d'une liste d'attributs avec transfert de blocs	712
Tableau F.6 – Exemple: écriture de la valeur d'un attribut unique sans transfert de blocs	715
Tableau F.7 – Exemple: écriture de la valeur d'une liste d'attributs sans transfert de blocs	716
Tableau F.8 – Exemple: écriture de la valeur d'un attribut unique avec transfert de blocs	718
Tableau F.9 – Exemple: écriture de la valeur d'une liste d'attributs avec transfert de blocs	720
Tableau F.10 – Exemple: service ACCESS sans transfert de bloc général	723
Tableau F.11 – Tampon "Profile generic" – get-response avec codage normal	730
Tableau F.12 – Tampon "Profile generic" – get-response avec compression null-data	732
Tableau F.13 – Tampon "Profile generic" – get-response avec codage compact-array	735
Tableau F.14 – Tampon "Profile generic" – get-response avec codage null-data et delta-value	738
Tableau F.15 – Comparaison de différentes méthodes de codage pour l'APDU get-response	740
Tableau F.16 – Combinaison des différentes méthodes de codage et compression V.44 pour l'APDU get-response	741
Tableau G.1 – ECC_P256_Domain_Parameters	742
Tableau G.2 – ECC_P384_Domain_Parameters	743
Tableau H.1 – Champs des certificats de clé publique utilisant P-256 signé avec P-256	744
Tableau I.1 – Vecteur d'essai pour agrément de clé utilisant le schéma Ephemeral Unified Model C(2e, 0s, ECC CDH)	748
Tableau I.2 – Vecteur d'essai pour agrément de clé utilisant le schéma One-pass Diffie-Hellman (1e, 1s, ECC CDH)	751
Tableau I.3 – Vecteur d'essai pour agrément de clé utilisant le schéma de modèle unifié statique (0e, 2s, ECC CDH)	755

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 du présent document 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.

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

Cette quatrième édition annule et remplace la troisième édition parue en 2017. Cette édition constitue une révision technique.

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

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
13/1890/FDIS	13/1904/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

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

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

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*, se trouve sur le site Web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site Web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT — Le logo "colour inside" qui se trouve sur la page de couverture de ce document 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.

INTRODUCTION

Cette quatrième 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 A.

La présente édition est conforme à DLMS® UA 1000-2, the "Green Book" Ed. 10:2020 et DLMS® UA 1000-2, the "Green Book" Ed. 10 Amendment 1 2021.

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les 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, la validité et 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 à des demandeurs du monde entier, en des termes et à des conditions raisonnables et non discriminatoires. À cet égard, la déclaration du fournisseur du service de maintenance est enregistrée à l'IEC. Des informations peuvent être obtenues auprès de:

DLMS¹ User Association (Association des utilisateurs de la DLMS)
www.dlms.com

¹ Device Language Message Specification (Spécification des messages de langage d'équipement).

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 concernant la structure, les services et les 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 62056-6-2:2021, 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 le matériel de comptage 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 le système de messages courts (SMS, Short Message Service).

L'Annexe C (normative) spécifie le protocole de 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 protégés entre une tierce partie et un serveur.

L'Annexe K (informative) énumère les modifications techniques majeures contenues dans cette quatrième édition.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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, *Lecture des compteurs électriques – Glossaire de termes*

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 62056-6-2:2021, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 6-2:Classes d'interfaces COSEM*

IEC 62056-7-3:2017, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 7-3: Profils de communication M-Bus filaire et sans fil pour les réseaux locaux et les réseaux de voisinage*

IEC 62056-7-6:2013, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 7-6:Profil de communication à 3 couches, orienté connexion et basé sur HDLC*

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*

IEC 62056-8-11:–² *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-11:Communication profile for Wi-SUN field area mesh networks* (disponible en anglais seulement)

IEC 62056-8-12:–³ *Electricity metering data exchange – The DLMS®/COSEM suite – Part 8-12:Communication profile for Low Power Wide Area Networks (LPWAN)* (disponible en anglais seulement)

IEC 62056-9-7:2013, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 9-7:Profil de communication pour réseaux TCP-UDP/IP*

ISO/IEC 8824-1:2008, *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1) – Partie 1:Spécification de la notation de base*

ISO/IEC 8825-1:2008, *Technologies de l'information – Règles de codage ASN.1 – Partie 1:Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)*

² En cours d'élaboration. Stade au moment de la publication: IEC CDV.

³ En cours d'élaboration. Stade au moment de la publication: 13/1877/CDV:2023.

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 ainsi que ses amendements A1:1997 et A2:1998, 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 ainsi que ses amendements A1:1997 et A2:1998, dont elle constitue une révision technique.

ISO/IEC 7498-1:1994, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base:le modèle de base*

UIT-T X.509:2008, *SÉRIE X:RÉSEAUX DE DONNÉES ET 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 (SHS)* (disponible en anglais seulement)

FIPS PUB 186-4:2013, *Digital Signature Standard (DSS)* (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 800-56A 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)

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

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

SEC1:2009, *Standards for Efficient Cryptography:Elliptic Curve Cryptography* (disponible en anglais seulement).SECG. Version 2.0

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Éditée par J. Schaad (Soaring Hawk Consulting) et R. Housley (RSA Laboratories), septembre 2002, <http://tools.ietf.org/html/rfc3394>

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)* <http://www.rfc-editor.org/rfc/rfc4106.txt>

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

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