

# 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 978-2-8322-3019-0

**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.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references .....	11
3 Terms, definitions and abbreviations .....	13
3.1 Terms and definitions .....	13
3.2 Abbreviations .....	13
4 Overview .....	15
4.1 DLMS/COSEM application layer structure .....	15
4.2 DLMS/COSEM application layer services.....	16
4.2.1 ASO services .....	16
4.2.2 Services provided for application association establishment and release .....	16
4.2.3 Services provided for data transfer .....	17
4.2.4 Layer management services .....	22
4.2.5 Summary of DLMS/COSEM application layer services .....	22
4.3 DLMS/COSEM application layer protocols .....	22
5 Information security in DLMS/COSEM .....	23
5.1 Definitions.....	23
5.2 General.....	23
5.3 Data access security .....	24
5.3.1 Overview .....	24
5.3.2 No security (lowest level security) authentication .....	24
5.3.3 Low Level Security (LLS) authentication .....	24
5.3.4 High Level Security (HLS) authentication .....	25
5.4 Data transport security .....	27
5.4.1 Applying, removing or checking the protection: ciphering and deciphering.....	27
5.4.2 Security context .....	28
5.4.3 Security policy .....	28
5.4.4 Security suite .....	29
5.4.5 Security material .....	29
5.4.6 Ciphered xDLMS APDUs.....	29
5.4.7 Cryptographic keys .....	31
5.4.8 The Galois/Counter Mode of Operation (GCM).....	34
6 DLMS/COSEM application layer service specification .....	43
6.1 Service primitives and parameters .....	43
6.2 The COSEM-OPEN service .....	45
6.3 The COSEM-RELEASE service .....	50
6.4 COSEM-ABORT service .....	52
6.5 Protection and general block transfer parameters .....	53
6.6 The GET service .....	57
6.7 The SET service .....	59
6.8 The ACTION service .....	62
6.9 The DataNotification service.....	66
6.10 The EventNotification service .....	67
6.11 The TriggerEventNotificationSending service .....	68

6.12	Variable access specification.....	69
6.13	The Read service.....	69
6.14	The Write service.....	73
6.15	The UnconfirmedWrite service.....	76
6.16	The InformationReport service.....	77
6.17	Client side layer management services: the SetMapperTable.request.....	78
6.18	Summary of services and LN/SN data transfer service mapping.....	78
7	DLMS/COSEM application layer protocol specification.....	79
7.1	The control function.....	79
7.1.1	State definitions of the client side control function.....	79
7.1.2	State definitions of the server side control function.....	81
7.2	The ACSE services and APDUs.....	82
7.2.1	ACSE functional units, services and service parameters.....	82
7.2.2	Registered COSEM names.....	85
7.2.3	APDU encoding rules.....	87
7.2.4	Protocol for application association establishment.....	87
7.2.5	Protocol for application association release.....	92
7.3	Protocol for the data transfer services.....	95
7.3.1	Negotiation of services and options – the conformance block.....	95
7.3.2	Confirmed and unconfirmed service invocations.....	96
7.3.3	Protocol for the GET service.....	98
7.3.4	Protocol for the SET service.....	101
7.3.5	Protocol for the ACTION service.....	104
7.3.6	Protocol of the DataNotification service.....	106
7.3.7	Protocol for the EventNotification service.....	106
7.3.8	Protocol for the Read service.....	106
7.3.9	Protocol for the Write service.....	110
7.3.10	Protocol for the UnconfirmedWrite service.....	114
7.3.11	Protocol for the InformationReport service.....	115
7.3.12	Protocol of general block transfer mechanism.....	116
8	Abstract syntax of ACSE and COSEM APDUs.....	127
Annex A (normative) Using the COSEM application layer in various communications profiles.....		142
A.1	General.....	142
A.2	Targeted communication environments.....	142
A.3	The structure of the profile.....	142
A.4	Identification and addressing schemes.....	142
A.5	Supporting layer services and service mapping.....	143
A.6	Communication profile specific parameters of the COSEM AL services.....	143
A.7	Specific considerations / constraints using certain services within a given profile.....	143
A.8	The 3-layer, connection-oriented, HDLC based communication profile.....	143
A.9	The TCP-UDP/IP based communication profiles (COSEM_on_IP).....	143
A.10	The S-FSK PLC profile.....	143
Annex B (normative) SMS short wrapper.....		144
Annex C (informative) AARQ and AARE encoding examples.....		145
C.1	General.....	145
C.2	Encoding of the xDLMS InitiateRequest / InitiateResponse APDUs.....	145
C.3	Specification of the AARQ and AARE APDUs.....	148

C.4	Data for the examples .....	149
C.5	Encoding of the AARQ APDU .....	150
C.6	Encoding of the AARE APDU.....	153
Annex D (informative) Encoding examples: AARQ and AARE APDUs using a ciphered application context.....		159
D.1	A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key .....	159
D.2	Authenticated encryption of the xDLMS InitiateRequest APDU .....	160
D.3	The AARQ APDU .....	161
D.4	A-XDR encoding of the xDLMS InitiateResponse APDU .....	162
D.5	Authenticated encryption of the xDLMS InitiateResponse APDU .....	163
D.6	The AARE APDU.....	164
D.7	The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU).....	165
D.8	The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU).....	166
Annex E (informative) Data transfer service examples .....		167
Annex F (informative) Overview of cryptography.....		183
F.1	General.....	183
F.2	Hash functions .....	183
F.3	Symmetric key algorithms.....	184
F.3.1	General .....	184
F.3.2	Encryption and decryption .....	184
F.3.3	Advanced Encryption Standard (AES).....	185
F.3.4	Encryption Modes of Operation .....	185
F.3.5	Message Authentication Code .....	186
F.3.6	Key establishment.....	187
F.4	Asymmetric key algorithms.....	187
F.4.1	General .....	187
F.4.2	Digital signatures .....	188
F.4.3	Key establishment.....	188
Annex G (informative) Significant technical changes with respect to IEC 62056-5-3 Ed.1.0:2013.....		189
Bibliography.....		191
Index.....		194
Figure 1 – Structure of the COSEM Application layers .....		15
Figure 2 – Summary of DLMS/COSEM AL services.....		22
Figure 3 – Authentication mechanisms during AA establishment .....		27
Figure 4 – Structure of service specific global ciphering and dedicated ciphering APDUs .....		30
Figure 5 – Structure of general global ciphering and dedicated ciphering APDUs .....		30
Figure 6 – Cryptographic protection of xDLMS APDUs using GCM.....		37
Figure 7 – Service primitives.....		43
Figure 8 – Time sequence diagrams.....		44
Figure 9 – Additional service parameters to control cryptographic protection and general block transfer .....		54
Figure 10 – Partial state machine for the client side control function .....		80
Figure 11 – Partial state machine for the server side control function .....		81

Figure 12 – MSC for successful AA establishment preceded by a successful lower layer connection establishment .....	88
Figure 13 – Graceful AA release using the A-RELEASE service .....	93
Figure 14 – Graceful AA release by disconnecting the supporting layer .....	94
Figure 15 – Aborting an AA following a PH-ABORT indication .....	95
Figure 16 – MSC of the GET service .....	98
Figure 17 – MSC of the GET service with block transfer .....	99
Figure 18 – MSC of the GET service with block transfer, long GET aborted .....	101
Figure 19 – MSC of the SET service .....	102
Figure 20 – MSC of the SET service with block transfer .....	102
Figure 21 – MSC of the ACTION service .....	104
Figure 22 – MSC of the ACTION service with block transfer .....	105
Figure 23 – MSC of the Read service used for reading an attribute .....	109
Figure 24 – MSC of the Read service used for invoking a method .....	109
Figure 25 – MSC of the Read Service used for reading an attribute, with block transfer .....	110
Figure 26 – MSC of the Write service used for writing an attribute .....	113
Figure 27 – MSC of the Write service used for invoking a method .....	113
Figure 28 – MSC of the Write service used for writing an attribute, with block transfer .....	114
Figure 29 – MSC of the Unconfirmed Write service used for writing an attribute .....	115
Figure 30 – Partial service invocations and GBT APDUs .....	118
Figure 31 – GET service with GBT, switching to streaming .....	120
Figure 32 – GET service with partial invocations, GBT and streaming, recovery of 4 <sup>th</sup> block sent in the 2nd stream .....	121
Figure 33 – GET service with partial invocations, GBT and streaming, recovery of 4 <sup>th</sup> and 5 <sup>th</sup> blocks .....	122
Figure 34 – GET service with partial invocations, GBT and streaming, recovery of last block .....	123
Figure 35 – SET service with GBT, with server not supporting streaming, recovery of 3rd block .....	124
Figure 36 – ACTION-WITH-LIST service with bi-directional GBT and block recovery .....	125
Figure 37 – DataNotification service with GBT with partial invocation .....	126
Figure B.1 – Short wrapper .....	144
Figure F.1 – Hash function .....	184
Figure F.2 – Encryption and decryption .....	185
Figure F.3 – Message Authentication Codes (MACs) .....	186
Table 1 – Clarification of the meaning of PDU Size for DLMS/COSEM .....	18
Table 2 – Security suites .....	29
Table 3 – Ciphered xDLMS APDUs .....	29
Table 4 – Use of the fields of the ciphered APDUs .....	31
Table 5 – Cryptographic keys and their management .....	34
Table 6 – Security control byte .....	38
Table 7 – Plaintext and additional authenticated data .....	38
Table 8 – Example for ciphered APDUs .....	40
Table 9 – HLS example with GMAC .....	42

Table 10 – Codes for AL service parameters .....	45
Table 11 – Service parameters of the COSEM-OPEN service primitives .....	46
Table 12 – Service parameters of the COSEM-RELEASE service primitives .....	50
Table 13 – Service parameters of the COSEM-ABORT service primitives .....	53
Table 14 – Additional service parameters .....	55
Table 15 – Security parameters .....	56
Table 16 – Service parameters of the GET service .....	57
Table 17 – GET service request and response types .....	58
Table 18 – Service parameters of the SET service .....	60
Table 19 – SET service request and response types .....	61
Table 20 – Service parameters of the ACTION service .....	63
Table 21 – ACTION service request and response types .....	64
Table 22 – Service parameters of the DataNotification service primitives .....	66
Table 23 – Service parameters of the EventNotification service primitives .....	67
Table 24 – Service parameters of the TriggerEventNotificationSending.request service primitive .....	68
Table 25 – Variable Access Specification .....	69
Table 26 – Service parameters of the Read service .....	70
Table 27 – Use of the Variable_Access_Specification variants and the Read.response choices .....	71
Table 28 – Service parameters of the Write service .....	74
Table 29 – Use of the Variable_Access_Specification variants and the Write.response choices .....	74
Table 30 – Service parameters of the UnconfirmedWrite service .....	76
Table 31 – Use of the Variable_Access_Specification variants .....	77
Table 32 – Service parameters of the InformationReport service .....	78
Table 33 – Service parameters of the SetMapperTable.request service primitives .....	78
Table 34 – Summary of ACSE services .....	79
Table 35 – Summary of xDLMS services for LN referencing .....	79
Table 36 – Summary of xDLMS services for SN referencing .....	79
Table 37 – ACSE functional units, services and service parameters .....	83
Table 38 – Use of ciphered / unciphered APDUs .....	86
Table 39 – xDLMS Conformance block .....	96
Table 40 – GET service types and APDUs .....	98
Table 41 – SET service types and APDUs .....	101
Table 42 – ACTION service types and APDUs .....	104
Table 43 – Mapping between the GET and the Read services .....	107
Table 44 – Mapping between the ACTION and the Read services .....	108
Table 45 – Mapping between the SET and the Write services .....	111
Table 46 – Mapping between the ACTION and the Write service .....	112
Table 47 – Mapping between the SET and the UnconfirmedWrite services .....	115
Table 48 – Mapping between the ACTION and the UnconfirmedWrite services .....	115
Table 49 – Mapping between the EventNotification and InformationReport services .....	116
Table B.1 – Reserved Application Processes .....	144

Table C.1 – Conformance block .....	146
Table C.2 – A-XDR encoding of the xDLMS InitiateRequest APDU.....	147
Table C.3 – A-XDR encoding of the xDLMS InitiateResponse APDU .....	148
Table C.4 – BER encoding of the AARQ APDU.....	151
Table C.5 – Complete AARQ APDU .....	153
Table C.6 – BER encoding of the AARE APDU .....	154
Table C.7 – The complete AARE APDU.....	158
Table D.1 – A-XDR encoding of the xDLMS InitiateRequest APDU.....	159
Table D.2 – Authenticated encryption of the xDLMS InitiateRequest APDU .....	160
Table D.3 – BER encoding of the AARQ APDU.....	161
Table D.4 – A-XDR encoding of the xDLMS InitiateResponse APDU .....	163
Table D.5 – Authenticated encryption of the xDLMS InitiateResponse APDU.....	163
Table D.6 – BER encoding of the AARE APDU .....	164
Table D.7 – BER encoding of the RLRQ APDU .....	166
Table D.8 – BER encoding of the RLRE APDU .....	166
Table E.1 – Objects used in the examples .....	167
Table E.2 – Example: Reading the value of a single attribute without block transfer .....	168
Table E.3 – Example: Reading the value of a list of attributes without block transfer.....	169
Table E.4 – Example: Reading the value of a single attribute with block transfer .....	171
Table E.5 – Example: Reading the value of a list of attributes with block transfer .....	173
Table E.6 – Example: Writing the value of a single attribute without block transfer .....	176
Table E.7 – Example: Writing the value of a list of attributes without block transfer .....	177
Table E.8 – Example: Writing the value of a single attribute with block transfer .....	178
Table E.9 – Example: Writing the value of a list of attributes with block transfer .....	180



## INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

#### Part 5-3: DLMS/COSEM application layer

#### FOREWORD

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

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

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

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

DLMS<sup>1</sup> User Association  
Zug/Switzerland  
www.dlms.com

---

<sup>1</sup> Device Language Message Specification.



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

This second edition cancels and replaces the first edition of IEC 62056-5-3 published in 2013. It constitutes a technical revision.

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

The text of this standard is based on the following documents:

FDIS	Report on voting
13/1648/FDIS	13/1657/RVD

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

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

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

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

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

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

## INTRODUCTION

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

This edition is in line with the DLMS UA Green Book Edition 7.0 Amendment 3. The main new features are the DataNotification service, the general protection and the general block transfer mechanisms and the SMS short wrapper.

In 2014, the DLMS UA has published Green Book Edition 8.0 adding several new features regarding functionality, efficiency and security while keeping full backwards compatibility.

The intention of the DLMS UA is to bring also these latest developments to international standardization. Therefore, IEC TC13 WG14 launched a project to bring these new elements also to the IEC 62056 series that will lead to Edition 3.0 of the standard.

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

Withdrawn

## **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 COSEM clients and servers, and defines how to use the DLMS/COSEM application layer in various 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 62056-6-2:2016, 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, Annex D and Annex E (informative) include encoding examples for APDUs.

Annex F (informative) provides an overview of cryptography.

Annex G (informative) lists the main technical changes in this edition of the standard.

#### **2 Normative references**

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 62056-1-0, *Electricity metering data exchange – The DLMS/COSEM suite – Part 1-0: Smart metering standardisation framework*

IEC 62056-6-1:2015, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-1: Object Identification System (OBIS)*

IEC 62056-6-2:2016, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*

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

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

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

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

NOTE This standard cancels and replaces ISO/IEC 8649-1:1999 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.

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

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

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

NIST SP 800-57:2006, *Recommendation for Key Management – Part 1: General (Revised)*

The following RFCs are available online from the Internet Engineering Task Force (IETF):  
<http://www.ietf.org/rfc/std-index.txt>, <http://www.ietf.org/rfc/>

RFC 1321, *The MD5 Message-Digest Algorithm*. Edited by R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.) April 1992

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*

## SOMMAIRE

AVANT-PROPOS.....	204
INTRODUCTION.....	206
1 Domaine d'application .....	207
2 Références normatives .....	207
3 Termes, définitions et abréviations.....	209
3.1 Termes et définitions.....	209
3.2 Abréviations.....	209
4 Vue d'ensemble.....	211
4.1 Structure de la couche application DLMS/COSEM.....	211
4.2 Services de la couche application DLMS/COSEM .....	213
4.2.1 Services ASO .....	213
4.2.2 Services fournis pour l'établissement et la libération d'associations d'applications.....	213
4.2.3 Services fournis pour le transfert de données.....	214
4.2.4 Services de gestion de couche.....	219
4.2.5 Récapitulatif des services de la couche application DLMS/COSEM .....	219
4.3 Protocoles de la couche application DLMS/COSEM .....	220
5 Sécurité des informations dans DLMS/COSEM.....	221
5.1 Définitions.....	221
5.2 Généralités.....	221
5.3 Sécurité de l'accès aux données.....	222
5.3.1 Vue d'ensemble .....	222
5.3.2 Authentification sans sécurité (niveau de sécurité le plus faible) .....	222
5.3.3 Authentification de niveau de sécurité faible (LLS).....	222
5.3.4 Authentification de niveau de sécurité élevé (HLS) .....	223
5.4 Sécurité de transport des données .....	226
5.4.1 Application, suppression ou vérification de la protection: chiffrement et déchiffrement.....	226
5.4.2 Contexte de sécurité .....	227
5.4.3 Politique de sécurité.....	227
5.4.4 Suite de sécurité.....	228
5.4.5 Matériel de sécurité.....	228
5.4.6 APDU xDLMS chiffrées .....	228
5.4.7 Clés cryptographiques.....	231
5.4.8 Mode de fonctionnement Galois/Counter (GCM) .....	235
6 Spécification de service de la couche application DLMS/COSEM.....	244
6.1 Primitives de service et paramètres .....	244
6.2 Service COSEM-OPEN .....	247
6.3 Service COSEM-RELEASE.....	252
6.4 Service COSEM-ABORT .....	255
6.5 Paramètres de protection et de transfert général de blocs.....	255
6.6 Service GET .....	260
6.7 Service SET.....	263
6.8 Service ACTION.....	266
6.9 Service DataNotification .....	269
6.10 Service EventNotification.....	270

6.11	Service TriggerEventNotificationSending .....	272
6.12	Spécification d'accès variable.....	272
6.13	Service Read .....	273
6.14	Service Write .....	277
6.15	Service UnconfirmedWrite .....	280
6.16	Service InformationReport.....	282
6.17	Services de gestion de couches côté client: Demande SetMapperTable.request .....	283
6.18	Récapitulatif des services et de la mise en correspondance de services de transfert de données LN/SN .....	283
7	Spécification du protocole de couche application DLMS/COSEM .....	284
7.1	Fonction de commande .....	284
7.1.1	Définitions des états de la fonction de commande côté client .....	284
7.1.2	Définitions des états de la fonction de commande côté serveur .....	286
7.2	Services ACSE et APDU .....	287
7.2.1	Unités fonctionnelles ACSE, services et paramètres de service.....	287
7.2.2	Noms COSEM enregistrés.....	290
7.2.3	Règles de codage d'APDU .....	292
7.2.4	Protocole d'établissement d'association d'applications.....	292
7.2.5	Protocole de libération d'association d'applications.....	298
7.3	Protocole des services de transfert de données .....	303
7.3.1	Négociation de services et d'options – Bloc de conformité.....	303
7.3.2	Appels de service confirmés et non confirmés.....	304
7.3.3	Protocole du service GET.....	305
7.3.4	Protocole du service SET.....	310
7.3.5	Protocole du service ACTION.....	314
7.3.6	Protocole du service DataNotification .....	317
7.3.7	Protocole du service EventNotification.....	317
7.3.8	Protocole du service Read.....	317
7.3.9	Protocole du service Write.....	322
7.3.10	Protocole du service UnconfirmedWrite .....	326
7.3.11	Protocole du service InformationReport .....	328
7.3.12	Protocole du mécanisme de transfert général de blocs.....	329
8	Syntaxe abstraite des APDU ACSE et COSEM.....	345
Annexe A (normative) Utilisation de la couche application COSEM dans différents profils de communication .....		360
A.1	Généralités .....	360
A.2	Environnements de communication ciblés.....	360
A.3	Structure du profil .....	360
A.4	Schéma d'identification et d'adressage .....	360
A.5	Services de couche de support et mise en correspondance de services .....	361
A.6	Paramètres spécifiques au profil de communication des services d'AL COSEM .....	361
A.7	Considérations / contraintes spécifiques à l'utilisation de certains services dans un profil donné.....	361
A.8	Profil de communication à 3 couches, orienté connexion et basé sur HDLC.....	361
A.9	Profils de communication basés sur TCP-UDP/IP (COSEM_on_IP) .....	361
A.10	Profil S-FSK PLC .....	361
Annexe B (normative) Emballage réduit pour SMS.....		362

Annexe C (informative) Exemples de codage AARQ et AARE .....	363
C.1 Généralités .....	363
C.2 Codage des APDU xDLMS InitiateRequest / InitiateResponse .....	363
C.3 Spécification des APDU AARQ et AARE .....	366
C.4 Données pour les exemples .....	367
C.5 Codage de l'APDU AARQ .....	368
C.6 Codage de l'APDU AARE .....	371
Annexe D (informative) Exemples de codage: APDU AARQ et AARE utilisant un contexte d'application chiffré .....	377
D.1 Codage A-XDR de l'APDU xDLMS InitiateRequest contenant une clé dédiée .....	377
D.2 Chiffrement authentifié de l'APDU xDLMS InitiateRequest .....	378
D.3 APDU AARQ .....	379
D.4 Codage A-XDR de l'APDU xDLMS InitiateResponse .....	380
D.5 Chiffrement authentifié de l'APDU xDLMS InitiateResponse .....	381
D.6 APDU AARQ .....	382
D.7 APDU RLRQ (contenant une APDU xDLMS InitiateRequest chiffrée) .....	383
D.8 APDU RLRE (contenant une APDU xDLMS InitiateResponse chiffrée) .....	384
Annexe E (informative) Exemples de services de transfert de données .....	385
Annexe F (informative) Présentation de la cryptographie .....	401
F.1 Généralités .....	401
F.2 Fonctions de hachage .....	401
F.3 Algorithmes de clé symétrique .....	402
F.3.1 Généralités .....	402
F.3.2 Chiffrement et déchiffrement .....	402
F.3.3 Advanced Encryption Standard (AES) .....	403
F.3.4 Mode de fonctionnement du chiffrement .....	404
F.3.5 Code d'authentification de message .....	404
F.3.6 Établissement de la clé .....	405
F.4 Algorithmes de clé asymétrique .....	405
F.4.1 Généralités .....	405
F.4.2 Signatures numériques .....	406
F.4.3 Établissement de la clé .....	407
Annexe G (informative) Modifications techniques majeures par rapport à l'IEC 62056- 5-3 Éd. 1.0:2013 .....	408
Bibliographie .....	410
Index .....	413
Figure 1 – Structure des couches application COSEM .....	212
Figure 2 – Récapitulatif des services de l'AL DLMS/COSEM .....	220
Figure 3 – Mécanismes d'authentification pendant l'établissement de l'AA .....	226
Figure 4 – Structure d'APDU de chiffrement global et de chiffrement dédié spécifiques au service .....	229
Figure 5 – Structure d'APDU de chiffrement général global et de chiffrement général dédié .....	230
Figure 6 – Protection cryptographique des APDU xDLMS à l'aide de GCM .....	239
Figure 7 – Primitives de service .....	245
Figure 8 – Diagrammes de séquences temporelles .....	246



Figure 9 – Paramètres supplémentaires de service pour contrôler la protection cryptographique et le transfert général de blocs .....	257
Figure 10 – Diagramme d'états partiel pour la fonction de commande côté client.....	285
Figure 11 – Diagramme d'états partiel pour la fonction de commande côté serveur .....	286
Figure 12 – MSC pour l'établissement réussi d'une AA précédé de l'établissement réussi d'une connexion de couche inférieure de support .....	294
Figure 13 – Libération d'AA sans perte de données à l'aide du service A-RELEASE .....	299
Figure 14 – Libération d'AA sans perte de données par déconnexion de la couche de support.....	301
Figure 15 – Abandon d'une AA suite à la primitive PH-ABORT.indication .....	303
Figure 16 – MSC du service GET .....	306
Figure 17 – MSC du service GET avec transfert de bloc .....	307
Figure 18 – MSC du service GET avec transfert de bloc, GET long abandonné.....	310
Figure 19 – MSC du service SET .....	311
Figure 20 – MSC du service SET avec transfert de bloc.....	312
Figure 21 – MSC du service ACTION .....	315
Figure 22 – MSC du service ACTION avec transfert de bloc.....	316
Figure 23 – MSC du service Read utilisé pour lire un attribut.....	320
Figure 24 – MSC du service Read utilisé pour appeler une méthode .....	320
Figure 25 – MSC du service Read utilisé pour lire un attribut, avec transfert de blocs.....	321
Figure 26 – MSC du service Write utilisé pour écrire un attribut .....	325
Figure 27 – MSC du service Write utilisé pour appeler une méthode .....	325
Figure 28 – MSC du service Write utilisé pour écrire un attribut, avec transfert de blocs.....	326
Figure 29 – MSC du service Unconfirmed Write utilisé pour écrire un attribut .....	328
Figure 30 – Appels de service partiels et APDU GBT.....	331
Figure 31 – Service GET avec GBT, passage à la diffusion en flux .....	333
Figure 32 – Service GET avec appels partiels, GBT et diffusion en flux, récupération du 4 <sup>ème</sup> bloc envoyé dans le deuxième flux.....	335
Figure 33 – Service GET avec appels partiels, GBT et diffusion en flux, récupération des 4 <sup>ème</sup> et 5 <sup>ème</sup> blocs .....	337
Figure 34 – Service GET avec appels partiels, GBT et diffusion en flux, récupération du dernier bloc.....	339
Figure 35 – Service SET avec GBT, avec serveur ne prenant pas en charge la diffusion en flux, récupération du 3 <sup>ème</sup> bloc.....	340
Figure 36 – Service ACTION-WITH-LIST avec GBT bidirectionnel et récupération de blocs .....	342
Figure 37 – Service DataNotification avec GBT, avec appel partiel .....	344
Figure B.1 – Emballage réduit.....	362
Figure F.1 – Fonction de hachage .....	402
Figure F.2 – Chiffrement et déchiffrement.....	403
Figure F.3 – Codes d'authentification de message (MAC) .....	404
Tableau 1 – Explication de la signification des paramètres PDU Size pour DLMS/COSEM.....	215
Tableau 2 – Suites de sécurité.....	228
Tableau 3 – APDU xDLMS chiffrées.....	228

Tableau 4 – Utilisation des champs des APDU chiffrées .....	231
Tableau 5 – Clés cryptographiques et leur gestion.....	234
Tableau 6 – Octet de contrôle de sécurité .....	239
Tableau 7 – Texte brut et AAD .....	240
Tableau 8 – Exemple d'APDU chiffrées .....	242
Tableau 9 – Exemple HLS avec GMAC.....	244
Tableau 10 – Codes des paramètres de service de l'AL .....	247
Tableau 11 – Paramètres de service des primitives de service COSEM-OPEN .....	248
Tableau 12 – Paramètres de service des primitives de service COSEM-RELEASE .....	252
Tableau 13 – Paramètres de service des primitives de service COSEM-ABORT .....	255
Tableau 14 – Paramètres supplémentaires de service .....	257
Tableau 15 – Paramètres de sécurité .....	259
Tableau 16 – Paramètres de service du service GET .....	260
Tableau 17 – Types de demandes et de réponses du service GET .....	261
Tableau 18 – Paramètres du service SET .....	263
Tableau 19 – Types de demandes et de réponses du service SET .....	264
Tableau 20 – Paramètres du service ACTION .....	266
Tableau 21 – Types de demandes et de réponses du service ACTION .....	267
Tableau 22 – Paramètres de service des primitives de service DataNotification .....	270
Tableau 23 – Paramètres de service des primitives du service EventNotification .....	271
Tableau 24 – Paramètres de service de la primitive de service TriggerEventNotificationSending.request .....	272
Tableau 25 – Spécification d'accès variable .....	273
Tableau 26 – Paramètres du service Read .....	274
Tableau 27 – Utilisation des variantes du paramètre Variable_Access_Specification et des choix de Read.response .....	275
Tableau 28 – Paramètres du service Write .....	278
Tableau 29 – Utilisation des variantes de Variable_Access_Specification et des choix de Write.response.....	279
Tableau 30 – Paramètres du service UnconfirmedWrite .....	281
Tableau 31 – Utilisation des variantes de Variable_Access_Specification.....	281
Tableau 32 – Paramètres du service InformationReport .....	282
Tableau 33 – Paramètres de service des primitives de service SetMapperTable.request ....	283
Tableau 34 – Récapitulatif des services ACSE .....	283
Tableau 35 – Récapitulatif des services xDLMS pour le référencement LN.....	284
Tableau 36 – Récapitulatif des services xDLMS pour le référencement SN .....	284
Tableau 37 – Unités fonctionnelles ACSE, services et paramètres de service .....	288
Tableau 38 – Utilisation des APDU chiffrées et non chiffrées .....	291
Tableau 39 – Bloc de conformité xDLMS .....	304
Tableau 40 – Types et APDU de service GET.....	306
Tableau 41 – Types et APDU de service SET .....	311
Tableau 42 – Types et APDU de service ACTION .....	314
Tableau 43 – Mise en correspondance du service GET et du service Read .....	318
Tableau 44 – Mise en correspondance du service ACTION et du service Read .....	318

Tableau 45 – Mise en correspondance du service SET et du service Write.....	322
Tableau 46 – Mise en correspondance du service ACTION et du service Write.....	323
Tableau 47 – Mise en correspondance du service SET et du service UnconfirmedWrite .....	327
Tableau 48 – Mise en correspondance du service ACTION et du service UnconfirmedWrite .....	327
Tableau 49 – Mise en correspondance des services EventNotification et InformationReport.....	329
Tableau B.1 – Processus d’application réservés .....	362
Tableau C.1 – Bloc de conformité.....	364
Tableau C.2 – Codage A-XDR de l'APDU xDLMS InitiateRequest .....	365
Tableau C.3 – Codage A-XDR de l'APDU xDLMS InitiateResponse.....	366
Tableau C.4 – Codage BER de l'APDU AARQ .....	369
Tableau C.5 – APDU AARQ complète .....	371
Tableau C.6 – Codage BER de l'APDU AARE.....	372
Tableau C.7 – APDU AARE complète.....	376
Tableau D.1 – Codage A-XDR de l'APDU xDLMS InitiateRequest .....	377
Tableau D.2 – Chiffrement authentifié de l'APDU xDLMS InitiateRequest.....	378
Tableau D.3 – Codage BER de l'APDU AARQ .....	379
Tableau D.4 – Codage A-XDR de l'APDU xDLMS InitiateResponse.....	381
Tableau D.5 – Chiffrement authentifié de l'APDU xDLMS InitiateResponse .....	381
Tableau D.6 – Codage BER de l'APDU AARE.....	382
Tableau D.7 – Codage BER de l'APDU RLRO .....	384
Tableau D.8 – Codage BER de l'APDU RLRE.....	384
Tableau E.1 – Objets utilisés dans les exemples .....	385
Tableau E.2 – Exemple: Lecture de la valeur d'un attribut unique sans transfert de bloc.....	386
Tableau E.3 – Exemple: Lecture de la valeur d'une liste d'attributs sans transfert de bloc .....	387
Tableau E.4 – Exemple: Lecture de la valeur d'un attribut unique avec transfert de bloc.....	389
Tableau E.5 – Exemple: Lecture de la valeur d'une liste d'attributs avec transfert de bloc .....	391
Tableau E.6 – Exemple: Écriture de la valeur d'un attribut unique sans transfert de bloc ....	394
Tableau E.7 – Exemple: Écriture de la valeur d'une liste d'attributs sans transfert de bloc .....	395
Tableau E.8 – Exemple: Écriture de la valeur d'un attribut unique avec transfert de bloc ....	396
Tableau E.9 – Exemple: Écriture de la valeur d'une liste d'attributs avec transfert de bloc .....	398

## COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

#### Partie 5-3: Couche application DLMS/COSEM

##### AVANT-PROPOS

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

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité 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, à la validité et à la portée de ce service de maintenance.

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

DLMS<sup>1</sup> User Association  
Zug/Switzerland  
www.dlms.com

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

Cette deuxième édition annule et remplace la première édition de l'IEC 62056-5-3 parue en 2013. Cette édition constitue une révision technique.

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
13/1648/FDIS	13/1657/RVD

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

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

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

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

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

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

<sup>1</sup> Spécification de message de langage de dispositif.

## INTRODUCTION

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

Cette édition est conforme à l'Amendement 3 de l'édition 7.0 du Livre Vert de la DLMS UA. Les principales nouvelles fonctions sont le service DataNotification, la protection générale et les mécanismes de transfert général de blocs ainsi que l'emballage réduit pour SMS.

En 2014, la DLMS UA a publié l'édition 8.0 du Livre Vert, qui prévoit de nouvelles caractéristiques en matière de fonctionnalité, d'efficacité et de sécurité tout en maintenant une rétrocompatibilité totale.

En outre, l'intention de la DLMS UA est de mettre ces derniers développements en conformité avec la normalisation internationale. Par conséquent, le groupe de travail 14 du comité d'études 13 de l'IEC a lancé un projet visant à rendre conformes ces nouveaux éléments également à la série IEC 62056 en vue de présenter l'Édition 3.0 de la norme.

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

Withdrawn

## 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 indique la couche application DLMS/COSEM en termes de structure, de services et de protocoles pour les clients et serveurs COSEM, et définit comment utiliser la couche application DLMS/COSEM dans différents profils de communication.

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

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

L'Annexe B (normative) spécifie l'emballage réduit pour SMS.

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

L'Annexe F (informative) présente la cryptographie.

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

#### 2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

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



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

IEC 62056-1-0, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 1-0: Cadre de normalisation du comptage intelligent*

IEC 62056-6-1:2015, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 6-1: Système d'identification des objets (OBIS)*

IEC 62056-6-2:2016, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 6-2: Classes d'interface COSEM*

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

ISO/IEC 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*

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*

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

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

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

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

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

NIST SP 800-57:2006, *Recommendation for Key Management – Part 1: General* (Révisé)

Les références suivantes sont disponibles en ligne à partir du Internet Engineering Task Force (IETF, Groupe de travail d'ingénierie Internet): <http://www.ietf.org/rfc/std-index.txt>, <http://www.ietf.org/rfc/>

RFC 1321, *The MD5 Message-Digest Algorithm*. Édité par R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.) avril 1992

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Éditée par J. Schaad (Soaring Hawk Consulting) et R. Housley (RSA Laboratories) septembre 2002

RFC 4106:2005, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*