

# 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

PRICE CODE  
CODE PRIX

**XH**

ICS 17.220; 35.110; 91.140.50

ISBN 978-2-83220-812-0

**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.....                                                                          | 7  |
| 1 Scope.....                                                                           | 9  |
| 2 Normative references .....                                                           | 9  |
| 3 Terms, definitions and abbreviations .....                                           | 11 |
| 3.1 Terms and definitions .....                                                        | 11 |
| 3.2 Abbreviations .....                                                                | 11 |
| 4 Overview .....                                                                       | 13 |
| 4.1 COSEM application layer structure .....                                            | 13 |
| 4.2 COSEM application layer services.....                                              | 14 |
| 4.2.1 ASO services.....                                                                | 14 |
| 4.2.2 Services provided for application association establishment and<br>release ..... | 14 |
| 4.2.3 Services provided for data transfer .....                                        | 15 |
| 4.2.4 Layer management services .....                                                  | 19 |
| 4.2.5 Summary of COSEM application layer services .....                                | 19 |
| 4.3 COSEM application layer protocols .....                                            | 20 |
| 5 Information security in DLMS/COSEM .....                                             | 20 |
| 5.1 Definitions .....                                                                  | 20 |
| 5.2 General.....                                                                       | 20 |
| 5.3 Data access security .....                                                         | 21 |
| 5.3.1 Overview .....                                                                   | 21 |
| 5.3.2 Lowest level security (no security) .....                                        | 21 |
| 5.3.3 Low Level Security (LLS).....                                                    | 21 |
| 5.3.4 High Level Security (HLS) .....                                                  | 22 |
| 5.4 Data transport security .....                                                      | 23 |
| 5.4.1 Applying, removing or checking the protection: ciphering and<br>deciphering..... | 23 |
| 5.4.2 Security context.....                                                            | 25 |
| 5.4.3 Security policy .....                                                            | 25 |
| 5.4.4 Security suite .....                                                             | 25 |
| 5.4.5 Security material .....                                                          | 26 |
| 5.4.6 Ciphered xDLMS APDUs .....                                                       | 26 |
| 5.4.7 Cryptographic keys.....                                                          | 27 |
| 5.4.8 The Galois/Counter Mode of Operation (GCM) .....                                 | 30 |
| 6 COSEM application layer service specification .....                                  | 40 |
| 6.1 Service primitives and parameters.....                                             | 40 |
| 6.2 The COSEM-OPEN service .....                                                       | 42 |
| 6.3 The COSEM-RELEASE service .....                                                    | 47 |
| 6.4 COSEM-ABORT service .....                                                          | 49 |
| 6.5 Security parameters .....                                                          | 50 |
| 6.6 The GET service .....                                                              | 51 |
| 6.7 The SET service.....                                                               | 53 |
| 6.8 The ACTION service .....                                                           | 56 |
| 6.9 The EventNotification service .....                                                | 60 |
| 6.10 The TriggerEventNotificationSending service .....                                 | 61 |
| 6.11 Variable access specification .....                                               | 62 |
| 6.12 The Read service .....                                                            | 63 |

|                       |                                                                                  |     |
|-----------------------|----------------------------------------------------------------------------------|-----|
| 6.13                  | The Write service .....                                                          | 67  |
| 6.14                  | The UnconfirmedWrite service.....                                                | 70  |
| 6.15                  | The InformationReport service.....                                               | 71  |
| 6.16                  | Client side layer management services: the SetMapperTable.request.....           | 72  |
| 6.17                  | Summary of services and LN/SN data transfer service mapping .....                | 72  |
| 7                     | COSEM application layer protocol specification .....                             | 73  |
| 7.1                   | The control function.....                                                        | 73  |
| 7.1.1                 | State definitions of the client side control function .....                      | 73  |
| 7.1.2                 | State definitions of the server side control function .....                      | 75  |
| 7.2                   | The ACSE services and APDUs .....                                                | 76  |
| 7.2.1                 | ACSE functional units, services and service parameters.....                      | 76  |
| 7.2.2                 | Registered COSEM names .....                                                     | 79  |
| 7.2.3                 | APDU encoding rules .....                                                        | 81  |
| 7.2.4                 | Protocol for application association establishment.....                          | 81  |
| 7.2.5                 | Protocol for application association release .....                               | 85  |
| 7.3                   | Protocol for the data transfer services .....                                    | 89  |
| 7.3.1                 | Negotiation of services and options – the conformance block .....                | 89  |
| 7.3.2                 | Confirmed and unconfirmed service invocations .....                              | 90  |
| 7.3.3                 | Protocol for the GET service.....                                                | 91  |
| 7.3.4                 | Protocol for the SET service .....                                               | 94  |
| 7.3.5                 | Protocol for the ACTION service.....                                             | 97  |
| 7.3.6                 | Protocol for the EventNotification service .....                                 | 99  |
| 7.3.7                 | Protocol for the Read service .....                                              | 100 |
| 7.3.8                 | Protocol for the Write service.....                                              | 104 |
| 7.3.9                 | Protocol for the UnconfirmedWrite service .....                                  | 108 |
| 7.3.10                | Protocol for the InformationReport service .....                                 | 109 |
| 8                     | Abstract syntax of ACSE and COSEM APDUs .....                                    | 110 |
| Annex A (normative)   | Using the COSEM application layer in various communications profiles .....       | 124 |
| Annex B (informative) | AARQ and AARE encoding examples.....                                             | 126 |
| Annex C (informative) | Encoding examples: AARQ and AARE APDUs using a ciphered application context..... | 140 |
| Annex D (informative) | Data transfer service examples .....                                             | 148 |
| Annex E (informative) | Overview of cryptography .....                                                   | 163 |
| Annex F (informative) | Significant technical changes with respect to IEC 62056-53 .....                 | 169 |
| Bibliography          | .....                                                                            | 172 |
| Index                 | .....                                                                            | 174 |
| Figure 1              | – Structure of the COSEM Application layers .....                                | 13  |
| Figure 2              | – Summary of COSEM AL services .....                                             | 19  |
| Figure 3              | – LLS and HLS authentication .....                                               | 23  |
| Figure 4              | – Data transport security in DLMS/COSEM .....                                    | 24  |
| Figure 5              | – Ciphered xDLMS APDUs.....                                                      | 26  |
| Figure 6              | – Cryptographic protection of xDLMS APDUs using GCM.....                         | 33  |
| Figure 7              | – Service primitives.....                                                        | 40  |
| Figure 8              | – Time sequence diagrams .....                                                   | 41  |
| Figure 9              | – Partial state machine for the client side control function .....               | 74  |

|                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------|-----|
| Figure 10 – Partial state machine for the server side control function.....                                         | 75  |
| Figure 11 – MSC for successful AA establishment preceded by a successful lower layer connection establishment ..... | 82  |
| Figure 12 – Graceful AA release using the A-RELEASE service.....                                                    | 87  |
| Figure 13 – Graceful AA release by disconnecting the supporting layer .....                                         | 88  |
| Figure 14 – Aborting an AA following a PH-ABORT.indication .....                                                    | 89  |
| Figure 15 – MSC of the GET service.....                                                                             | 92  |
| Figure 16 – MSC of the GET service with block transfer .....                                                        | 92  |
| Figure 17 – MSC of the GET service with block transfer, long GET aborted .....                                      | 94  |
| Figure 18 – MSC of the SET service .....                                                                            | 95  |
| Figure 19 – MSC of the SET service with block transfer .....                                                        | 96  |
| Figure 20 – MSC of the ACTION service.....                                                                          | 98  |
| Figure 21 – MSC of the ACTION service with block transfer.....                                                      | 99  |
| Figure 22 – MSC of the Read service used for reading an attribute.....                                              | 102 |
| Figure 23 – MSC of the Read service used for invoking a method.....                                                 | 103 |
| Figure 24 – MSC of the Read Service used for reading an attribute, with block transfer .....                        | 104 |
| Figure 25 – MSC of the Write service used for writing an attribute .....                                            | 107 |
| Figure 26 – MSC of the Write service used for invoking a method.....                                                | 107 |
| Figure 27 – MSC of the Write Service used for writing an attribute, with block transfer .....                       | 108 |
| Figure 28 – MSC of the Unconfirmed Write service used for writing an attribute.....                                 | 109 |
| Figure E.1 – Hash function.....                                                                                     | 164 |
| Figure E.2 – Encryption and decryption.....                                                                         | 165 |
| Figure E.3 – Message Authentication Codes (MACs) .....                                                              | 166 |
| Table 1 – Clarification of the meaning of PDU Size for DLMS/COSEM .....                                             | 16  |
| Table 2 – Security suites .....                                                                                     | 26  |
| Table 3 – Security control field.....                                                                               | 27  |
| Table 4 – Cryptographic keys and their management.....                                                              | 30  |
| Table 5 – Plaintext and additional authenticated data .....                                                         | 34  |
| Table 6 – Example for ciphered APDUs .....                                                                          | 37  |
| Table 7 – HLS example with GMAC .....                                                                               | 39  |
| Table 8 – Codes for AL service parameters .....                                                                     | 42  |
| Table 9 – Service parameters of the COSEM-OPEN service primitives .....                                             | 43  |
| Table 10 – Service parameters of the COSEM-RELEASE service primitives .....                                         | 47  |
| Table 11 – Service parameters of the COSEM-ABORT service primitives .....                                           | 50  |
| Table 12 – Security parameters .....                                                                                | 50  |
| Table 13 – Service parameters of the GET service .....                                                              | 51  |
| Table 14 – GET service request and response types .....                                                             | 52  |
| Table 15 – Service parameters of the SET service.....                                                               | 54  |
| Table 16 – SET service request and response types.....                                                              | 55  |
| Table 17 – Service parameters of the ACTION service .....                                                           | 57  |
| Table 18 – ACTION service request and response types .....                                                          | 58  |
| Table 19 – Service parameters of the EventNotification service primitives .....                                     | 60  |

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| Table 20 – Service parameters of the TriggerEventNotificationSending.request service primitive ..... | 61  |
| Table 21 – Variable Access Specification .....                                                       | 63  |
| Table 22 – Service parameters of the Read service .....                                              | 64  |
| Table 23 – Use of the Variable_Access_Specification variants and the Read.response choices .....     | 65  |
| Table 24 – Service parameters of the Write service .....                                             | 68  |
| Table 25 – Use of the Variable_Access_Specification variants and the Write.response choices .....    | 68  |
| Table 26 – Service parameters of the UnconfirmedWrite service .....                                  | 70  |
| Table 27 – Use of the Variable_Access_Specification variants .....                                   | 71  |
| Table 28 – Service parameters of the InformationReport service .....                                 | 72  |
| Table 29 – Service parameters of the SetMapperTable.request service primitives .....                 | 72  |
| Table 30 – Summary of ACSE services .....                                                            | 73  |
| Table 31 – Summary of xDLMS services for LN referencing .....                                        | 73  |
| Table 32 – Summary of xDLMS services for SN referencing .....                                        | 73  |
| Table 33 – ACSE functional units, services and service parameters .....                              | 77  |
| Table 34 – Use of ciphered / unciphered APDUs .....                                                  | 80  |
| Table 35 – xDLMS Conformance block .....                                                             | 90  |
| Table 36 – GET service types and APDUs .....                                                         | 91  |
| Table 37 – SET service types and APDUs .....                                                         | 95  |
| Table 38 – ACTION service types and APDUs .....                                                      | 98  |
| Table 39 – Mapping between the GET and the Read services .....                                       | 100 |
| Table 40 – Mapping between the ACTION and the Read services .....                                    | 101 |
| Table 41 – Mapping between the SET and the Write services .....                                      | 105 |
| Table 42 – Mapping between the ACTION and the Write service .....                                    | 106 |
| Table 43 – Mapping between the SET and the UnconfirmedWrite services .....                           | 108 |
| Table 44 – Mapping between the ACTION and the UnconfirmedWrite services .....                        | 109 |
| Table 45 – Mapping between the EventNotification and InformationReport services .....                | 110 |
| Table B.1 – Conformance block .....                                                                  | 127 |
| Table B.2 – A-XDR encoding of the xDLMS InitiateRequest APDU .....                                   | 128 |
| Table B.3 – A-XDR encoding of the xDLMS InitiateResponse APDU .....                                  | 129 |
| Table B.4 – BER encoding of the AARQ APDU .....                                                      | 132 |
| Table B.5 – Complete AARQ APDU .....                                                                 | 134 |
| Table B.6 – BER encoding of the AARE APDU .....                                                      | 135 |
| Table B.7 – The complete AARE APDU .....                                                             | 139 |
| Table C.1 – A-XDR encoding of the xDLMS InitiateRequest APDU .....                                   | 140 |
| Table C.2 – Authenticated encryption of the xDLMS InitiateRequest APDU .....                         | 141 |
| Table C.3 – BER encoding of the AARQ APDU .....                                                      | 142 |
| Table C.4 – A-XDR encoding of the xDLMS InitiateResponse APDU .....                                  | 143 |
| Table C.5 – Authenticated encryption of the xDLMS InitiateResponse APDU .....                        | 144 |
| Table C.6 – BER encoding of the AARE APDU .....                                                      | 145 |
| Table C.7 – BER encoding of the RLRQ APDU .....                                                      | 146 |
| Table C.8 – BER encoding of the RLRE APDU .....                                                      | 147 |

|                                                                                             |     |
|---------------------------------------------------------------------------------------------|-----|
| Table D.1 – Objects used in the examples .....                                              | 148 |
| Table D.2 – Example: Reading the value of a single attribute without block transfer .....   | 149 |
| Table D.3 – Example: Reading the value of a list of attributes without block transfer ..... | 150 |
| Table D.4 – Example: Reading the value of a single attribute with block transfer .....      | 151 |
| Table D.5 – Example: Reading the value of a list of attributes with block transfer .....    | 153 |
| Table D.6 – Example: Writing the value of a single attribute without block transfer .....   | 155 |
| Table D.7 – Example: Writing the value of a list of attributes without block transfer ..... | 156 |
| Table D.8 – Example: Writing the value of a single attribute with block transfer .....      | 158 |
| Table D.9 – Example: Writing the value of a list of attributes with block transfer .....    | 160 |

## 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.ch](http://www.dlms.ch)

---

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

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

This edition cancels and replaces IEC 62056-53 published in 2006. It constitutes a technical revision.

The significant technical changes with respect to IEC 62056-53 are listed in Annex F.

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

|              |                  |
|--------------|------------------|
| FDIS         | Report on voting |
| 13/1523/FDIS | 13/1541/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.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The numbering scheme has changed from IEC 62056-XY to IEC 62056-X-Y. For example IEC 62056-53 becomes IEC 62056-5-3.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site 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.**

## **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<sup>2</sup>, 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, Annex C and Annex D (informative) include encoding examples for APDUs.

Annex E (informative) provides an overview of cryptography.

#### **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*

---

<sup>2</sup> To be published simultaneously with this part of IEC 62056.

IEC 62056-6-1:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-1: Object Identification System (OBIS)*<sup>3</sup>

IEC 62056-6-2:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*<sup>4</sup>

IEC 62056-8-3:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 8-3: Communication profile for PLC S-FSK neighbourhood networks*<sup>5</sup>

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

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

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)*

FIPS PUB 180-1:2002, *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)

RFC 1321:1992, Internet Engineering Task Force (IETF). *The MD5 Message-Digest Algorithm*. Edited by R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.) April 1992. Available from: <http://www.rfc-editor.org/rfc/rfc1321.txt>

RFC 3394:2002, Internet Engineering Task Force (IETF). *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002. Available from: <http://www.rfc-editor.org/rfc/rfc3394.txt>

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

NOTE See also the Bibliography.

---

<sup>3</sup> To be published simultaneously with this part of IEC 62056.

<sup>4</sup> To be published simultaneously with this part of IEC 62056.

<sup>5</sup> To be published simultaneously with this part of IEC 62056.

## SOMMAIRE

|                                                                                                     |     |
|-----------------------------------------------------------------------------------------------------|-----|
| AVANT-PROPOS .....                                                                                  | 183 |
| 1 Domaine d'application .....                                                                       | 185 |
| 2 Références normatives .....                                                                       | 185 |
| 3 Termes, définitions et abréviations .....                                                         | 187 |
| 3.1 Termes et définitions .....                                                                     | 187 |
| 3.2 Abréviations .....                                                                              | 187 |
| 4 Vue d'ensemble .....                                                                              | 189 |
| 4.1 Structure de la couche application COSEM .....                                                  | 189 |
| 4.2 Services de la couche application COSEM .....                                                   | 190 |
| 4.2.1 Services ASO .....                                                                            | 190 |
| 4.2.2 Services fournis pour l'établissement et la libération d'associations d'applications .....    | 190 |
| 4.2.3 Services fournis pour le transfert de données .....                                           | 191 |
| 4.2.4 Services de gestion de couche .....                                                           | 195 |
| 4.2.5 Récapitulatif des services de la couche application COSEM .....                               | 195 |
| 4.3 Protocoles de la couche application COSEM .....                                                 | 196 |
| 5 Sécurité des informations dans DLMS/COSEM .....                                                   | 196 |
| 5.1 Définitions .....                                                                               | 197 |
| 5.2 Généralités .....                                                                               | 197 |
| 5.3 Sécurité de l'accès aux données .....                                                           | 198 |
| 5.3.1 Vue d'ensemble .....                                                                          | 198 |
| 5.3.2 Niveau de sécurité le plus faible (pas de sécurité) .....                                     | 198 |
| 5.3.3 Niveau de sécurité faible (LLS) .....                                                         | 198 |
| 5.3.4 Niveau de Sécurité élevé (HLS) .....                                                          | 199 |
| 5.4 Sécurité de transport des données .....                                                         | 201 |
| 5.4.1 Application, suppression ou vérification de la protection: chiffrement et déchiffrement ..... | 201 |
| 5.4.2 Contexte de sécurité .....                                                                    | 203 |
| 5.4.3 Politique de sécurité .....                                                                   | 203 |
| 5.4.4 Suite de sécurité .....                                                                       | 204 |
| 5.4.5 Matériel de sécurité .....                                                                    | 204 |
| 5.4.6 APDU xDLMS chiffrées .....                                                                    | 204 |
| 5.4.7 Clés cryptographiques .....                                                                   | 206 |
| 5.4.8 Mode de fonctionnement Galois/Counter (GCM) .....                                             | 209 |
| 6 Spécification de service de la couche application COSEM .....                                     | 220 |
| 6.1 Primitives de service et paramètres .....                                                       | 220 |
| 6.2 Service COSEM-OPEN .....                                                                        | 224 |
| 6.3 Service COSEM-RELEASE .....                                                                     | 228 |
| 6.4 Service COSEM-ABORT .....                                                                       | 231 |
| 6.5 Paramètres de sécurité .....                                                                    | 231 |
| 6.6 Service GET .....                                                                               | 232 |
| 6.7 Service SET .....                                                                               | 235 |
| 6.8 Service ACTION .....                                                                            | 238 |
| 6.9 Service EventNotification .....                                                                 | 242 |
| 6.10 Service TriggerEventNotificationSending .....                                                  | 243 |
| 6.11 Spécification d'accès variable .....                                                           | 244 |

|        |                                                                                                                   |     |
|--------|-------------------------------------------------------------------------------------------------------------------|-----|
| 6.12   | Service Read.....                                                                                                 | 245 |
| 6.13   | Service Write.....                                                                                                | 249 |
| 6.14   | Service UnconfirmedWrite .....                                                                                    | 252 |
| 6.15   | Service InformationReport.....                                                                                    | 254 |
| 6.16   | Services de gestion de couches côté client: Demande<br>SetMapperTable.request .....                               | 255 |
| 6.17   | Récapitulatif des services et du mappage de service de transfert de données<br>LN/SN .....                        | 255 |
| 7      | Spécification du protocole de couche application COSEM .....                                                      | 256 |
| 7.1    | Fonction de commande .....                                                                                        | 256 |
| 7.1.1  | Définitions des états de la fonction de commande côté client .....                                                | 256 |
| 7.1.2  | Définitions des états de la fonction de commande côté serveur .....                                               | 258 |
| 7.2    | Services ACSE et APDU .....                                                                                       | 259 |
| 7.2.1  | Unités fonctionnelles ACSE, services et paramètres de service .....                                               | 259 |
| 7.2.2  | Noms COSEM enregistrés .....                                                                                      | 262 |
| 7.2.3  | Règles de codage d'APDU.....                                                                                      | 264 |
| 7.2.4  | Protocole d'établissement d'association d'applications .....                                                      | 264 |
| 7.2.5  | Protocole de libération d'association d'applications .....                                                        | 270 |
| 7.3    | Protocole des services de transfert de données .....                                                              | 276 |
| 7.3.1  | Négociation de services et d'options - Bloc de conformité.....                                                    | 276 |
| 7.3.2  | Appels de service confirmés et non confirmés .....                                                                | 277 |
| 7.3.3  | Protocole du service GET .....                                                                                    | 278 |
| 7.3.4  | Protocole du service SET .....                                                                                    | 283 |
| 7.3.5  | Protocole du service ACTION .....                                                                                 | 286 |
| 7.3.6  | Protocole du service EventNotification.....                                                                       | 289 |
| 7.3.7  | Protocole du service Read.....                                                                                    | 289 |
| 7.3.8  | Protocole du service Write.....                                                                                   | 293 |
| 7.3.9  | Protocole du service UnconfirmedWrite .....                                                                       | 297 |
| 7.3.10 | Protocole du service InformationReport .....                                                                      | 298 |
| 8      | Syntaxe abstraite des APDU ACSE et COSEM.....                                                                     | 299 |
|        | Annexe A (normative) Utilisation de la couche application COSEM dans différents<br>profils de communication ..... | 313 |
|        | Annexe B (informative) Exemples de codage AARQ et AARE .....                                                      | 315 |
|        | Annexe C (informative) Exemples de codage: APDU AARQ et AARE utilisant un<br>contexte d'application chiffré.....  | 328 |
|        | Annexe D (informative) Exemples de services de transfert de données.....                                          | 337 |
|        | Annexe E (informative) Présentation de la cryptographie .....                                                     | 353 |
|        | Annexe F (informative) Modifications techniques majeures par rapport à la CEI 62056-<br>53 .....                  | 360 |
|        | Bibliographie.....                                                                                                | 363 |
|        | Index .....                                                                                                       | 366 |
|        | Figure 1 – Structure des couches application COSEM .....                                                          | 189 |
|        | Figure 2 – Récapitulatif des services de l'AL COSEM .....                                                         | 196 |
|        | Figure 3 – Authentification LLS et HLS .....                                                                      | 201 |
|        | Figure 4 – Sécurité de transport des données dans DLMS/COSEM.....                                                 | 203 |
|        | Figure 5 – APDU xDLMS chiffrées .....                                                                             | 205 |
|        | Figure 6 – Protection cryptographique des APDU xDLMS à l'aide de GCM .....                                        | 215 |

|                                                                                                                                              |     |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 7 – Primitives de service .....                                                                                                       | 220 |
| Figure 8 – Diagrammes de séquences temporelles .....                                                                                         | 222 |
| Figure 9 – Machine à état, partielle, pour la fonction de commande côté client .....                                                         | 257 |
| Figure 10 – État partiel de la machine pour la fonction de commande côté serveur .....                                                       | 258 |
| Figure 11 – MSC pour l'établissement réussi d'une AA précédé de l'établissement réussi d'une connexion de couche inférieure de support ..... | 267 |
| Figure 12 – Libération d'AA sans perte de données à l'aide du service A-RELEASE .....                                                        | 272 |
| Figure 13 – Libération d'AA sans perte de données par déconnexion de la couche de support .....                                              | 274 |
| Figure 14 – Abandon d'une AA suite à la primitive PH-ABORT.indication .....                                                                  | 276 |
| Figure 15 – MSC du service GET .....                                                                                                         | 279 |
| Figure 16 – MSC du service GET avec transfert de bloc .....                                                                                  | 280 |
| Figure 17 – MSC du service GET avec transfert de bloc, GET long abandonné .....                                                              | 283 |
| Figure 18 – MSC du service SET .....                                                                                                         | 284 |
| Figure 19 – MSC du service SET avec transfert de bloc .....                                                                                  | 285 |
| Figure 20 – MSC du service ACTION .....                                                                                                      | 287 |
| Figure 21 – MSC du service ACTION avec transfert de bloc .....                                                                               | 288 |
| Figure 22 – MSC du service Read utilisé pour lire un attribut .....                                                                          | 292 |
| Figure 23 – MSC du service Read utilisé pour appeler une méthode .....                                                                       | 292 |
| Figure 24 – MSC du service Read utilisé pour lire un attribut, avec transfert de blocs .....                                                 | 293 |
| Figure 25 – MSC du service Write utilisé pour écrire un attribut .....                                                                       | 296 |
| Figure 26 – MSC du service Write utilisé pour appeler une méthode .....                                                                      | 296 |
| Figure 27 – MSC du service Write utilisé pour écrire un attribut, avec transfert de blocs .....                                              | 297 |
| Figure 28 – MSC du service Unconfirmed Write utilisé pour écrire un attribut .....                                                           | 298 |
| Figure E.1 – Fonction de hachage .....                                                                                                       | 354 |
| Figure E.2 – Chiffrement et déchiffrement .....                                                                                              | 355 |
| Figure E.3 – Codes d'authentification de message (MAC) .....                                                                                 | 356 |
| Tableau 1 – Explication de la signification des paramètres PDU Size pour DLMS/COSEM .....                                                    | 192 |
| Tableau 2 – Suites de sécurité .....                                                                                                         | 204 |
| Tableau 3 – Champ Security Control .....                                                                                                     | 206 |
| Tableau 4 – Clés cryptographiques et leur gestion .....                                                                                      | 209 |
| Tableau 5 – Texte brut et AAD .....                                                                                                          | 215 |
| Tableau 6 – Exemple d'APDU chiffrées .....                                                                                                   | 218 |
| Tableau 7 – Exemple HLS avec GMAC .....                                                                                                      | 219 |
| Tableau 8 – Codes des paramètres de service de l'AL .....                                                                                    | 223 |
| Tableau 9 – Paramètres de service des primitives de service COSEM-OPEN .....                                                                 | 224 |
| Tableau 10 – Paramètres de service des primitives de service COSEM-RELEASE .....                                                             | 228 |
| Tableau 11 – Paramètres de service des primitives de service COSEM-ABORT .....                                                               | 231 |
| Tableau 12 – Paramètres de sécurité .....                                                                                                    | 232 |
| Tableau 13 – Paramètres de service du service GET .....                                                                                      | 233 |
| Tableau 14 – Types de demande et de réponse du service GET .....                                                                             | 234 |

|                                                                                                                          |     |
|--------------------------------------------------------------------------------------------------------------------------|-----|
| Tableau 15 – Paramètres du service SET .....                                                                             | 236 |
| Tableau 16 – Types de demande et de réponse du service SET .....                                                         | 237 |
| Tableau 17 – Paramètres du service ACTION .....                                                                          | 239 |
| Tableau 18 – Types de demande et de réponse du service ACTION .....                                                      | 240 |
| Tableau 19 – Paramètres de service des primitives du service EventNotification .....                                     | 243 |
| Tableau 20 – Paramètres de service de la primitive de service<br>TriggerEventNotificationSending.request .....           | 244 |
| Tableau 21 – Spécification d'accès variable.....                                                                         | 245 |
| Tableau 22 – Paramètres du service Read.....                                                                             | 246 |
| Tableau 23 – Utilisation des variantes du paramètre Variable_Access_Specification et<br>des choix de Read.response ..... | 247 |
| Tableau 24 – Paramètres du service Write.....                                                                            | 250 |
| Tableau 25 – Utilisation des variantes de Variable_Access_Specification et des choix<br>de Write.response.....           | 251 |
| Tableau 26 – Paramètres du service UnconfirmedWrite .....                                                                | 253 |
| Tableau 27 – Utilisation des variantes de Variable_Access_Specification .....                                            | 253 |
| Tableau 28 – Paramètres du service InformationReport.....                                                                | 254 |
| Tableau 29 – Paramètres de service des primitives de service SetMapperTable.request ....                                 | 255 |
| Tableau 30 – Récapitulatif des services ACSE.....                                                                        | 255 |
| Tableau 31 – Récapitulatif des services xDLMS pour le référencement LN .....                                             | 256 |
| Tableau 32 – Récapitulatif des services xDLMS pour le référencement SN .....                                             | 256 |
| Tableau 33 – Unités fonctionnelles ACSE, services et paramètres de service .....                                         | 260 |
| Tableau 34 – Utilisation des APDU chiffrées et non chiffrées .....                                                       | 263 |
| Tableau 35 – Bloc de conformité xDLMS.....                                                                               | 276 |
| Tableau 36 – Types et APDU de service GET .....                                                                          | 278 |
| Tableau 37 – Types et APDU de service SET .....                                                                          | 283 |
| Tableau 38 – Types et APDU de service ACTION .....                                                                       | 286 |
| Tableau 39 – Mappage entre le service GET et le service Read .....                                                       | 290 |
| Tableau 40 – Mappage entre le service ACTION et le service Read.....                                                     | 290 |
| Tableau 41 – Mappage entre le service SET et le service Write .....                                                      | 294 |
| Tableau 42 – Mappage entre le service ACTION et le service Write.....                                                    | 295 |
| Tableau 43 – Mappage entre le service SET et le service UnconfirmedWrite .....                                           | 298 |
| Tableau 44 – Mappage entre le service ACTION et le service UnconfirmedWrite .....                                        | 298 |
| Tableau 45 – Mappage entre les services EventNotification et InformationReport .....                                     | 299 |
| Tableau B.1 – Bloc de conformité .....                                                                                   | 316 |
| Tableau B.3 – Codage A-XDR de l'APDU xDLMS InitiateResponse.....                                                         | 318 |
| Tableau B.4 – Codage BER de l'APDU AARQ.....                                                                             | 321 |
| Tableau B.5 – APDU AARQ complète .....                                                                                   | 323 |
| Tableau B.6 – Codage BER de l'APDU AARE .....                                                                            | 324 |
| Tableau B.7 – APDU AARE complète .....                                                                                   | 327 |
| Tableau C.1 – Codage A-XDR de l'APDU xDLMS InitiateRequest .....                                                         | 328 |
| Tableau C.2 – Chiffrement authentifié de l'APDU xDLMS InitiateRequest .....                                              | 329 |
| Tableau C.3 – Codage BER de l'APDU AARQ .....                                                                            | 330 |
| Tableau C.4 – Codage A-XDR de l'APDU xDLMS InitiateResponse .....                                                        | 332 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| Tableau C.5 – Chiffrement authentifié de l'APDU xDLMS InitiateResponse.....                       | 332 |
| Tableau C.6 – Codage BER de l'APDU AARE.....                                                      | 333 |
| Tableau C.7 – Codage BER de l'APDU RLRQ.....                                                      | 335 |
| Tableau C.8 – Codage BER de l'APDU RLRE.....                                                      | 336 |
| Tableau D.1 – Objets utilisés dans les exemples .....                                             | 337 |
| Tableau D.2 – Exemple: Lecture de la valeur d'un attribut unique sans transfert de bloc.....      | 338 |
| Tableau D.3 – Exemple: Lecture de la valeur d'une liste d'attributs sans transfert de bloc .....  | 339 |
| Tableau D.4 – Exemple: Lecture d'un attribut unique avec transfert de bloc.....                   | 340 |
| Tableau D.5 – Exemple: Lecture de la valeur d'une liste d'attributs avec transfert de bloc .....  | 343 |
| Tableau D.6 – Exemple: Écriture de la valeur d'un attribut unique sans transfert de bloc .....    | 346 |
| Tableau D.7 – Exemple: Écriture de la valeur d'une liste d'attributs sans transfert de bloc ..... | 347 |
| Tableau D.8 – Exemple: Écriture de la valeur d'un attribut unique avec transfert de bloc .....    | 348 |
| Tableau D.9 – Exemple: Écriture de la valeur d'une liste d'attributs avec transfert de bloc ..... | 350 |

## 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 Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de brevet. La CEI 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 (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité à la présente Norme internationale peut nécessiter l'utilisation d'un service de maintenance concernant la pile de protocoles sur laquelle est basée la présente Norme CEI 62056-5-3.

La CEI ne prend pas position concernant la preuve, la validité et le domaine d'application de ce service de maintenance.

Le fournisseur du service de maintenance a assuré à la CEI qu'il souhaite fournir des services aux demandeurs dans le monde entier, selon des termes et les conditions raisonnables et non discriminatoires. À cet égard, la déclaration du fournisseur du service de maintenance est enregistrée avec la CEI. Des informations peuvent être obtenues auprès de:

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

La Norme internationale CEI 62056-5-3 a été établie par le comité d'études 13 de la CEI: Mesure de l'énergie électrique, contrôle des tarifs et de la charge.

Cette édition annule et remplace la CEI 62056-53 parue en 2006. Cette édition constitue une révision technique.

Les modifications techniques majeures par rapport à la CEI 62056-53 sont énumérées dans l'Annexe F.

Le texte de cette norme est issu des documents suivants:

| FDIS         | Rapport de vote |
|--------------|-----------------|
| 13/1523/FDIS | 13/1541/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/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 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 la CEI.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

La numérotation est passée de CEI 62056-XY à CEI 62056-X-Y. Par exemple, la CEI 62056-53 devient la CEI 62056-5-3.

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 la CEI 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.

## **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 la CEI 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 la CEI 62056-6-2<sup>2</sup>, 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 CEI 62056.

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

L'Annexe E (informative) présente la cryptographie.

#### **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).

CEI 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*

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

CEI/TR 62051:1999, *Lecture des compteurs électriques – Glossaire de termes* (disponible en anglais seulement)

---

<sup>2</sup> A publier simultanément avec la présente partie de la CEI 62056.

CEI/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)

CEI 62056-6-1:—, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 6-1: Système d'identification des objets (OBIS)*<sup>3</sup>

CEI 62056-6-2:—, *Échange des données de comptage de l'électricité – La suite DLMS/COSEM – Partie 6-2: Classes d'interface COSEM*<sup>4</sup>

CEI 62056-8-3:—, *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*<sup>5</sup>

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

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

FIPS PUB 180-1:2002, *Secure hash standard* (disponible en anglais seulement)

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

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

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

RFC 1321:1992, Internet Engineering Task Force (IETF). *The MD5 Message-Digest Algorithm*. Édité par R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.) avril 1992. Disponible à l'adresse: <http://www.rfc-editor.org/rfc/rfc1321.txt> (disponible en anglais seulement)

RFC 3394:2002, Internet Engineering Task Force (IETF). *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Édité par J. Schaad (Soaring Hawk Consulting) et R. Housley (RSA Laboratories) septembre 2002. Disponible à l'adresse: <http://www.rfc-editor.org/rfc/rfc3394.txt> (disponible en anglais seulement)

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

<sup>3</sup> À publier simultanément avec la présente partie de la CEI 62056.

<sup>4</sup> À publier simultanément avec la présente partie de la CEI 62056.

<sup>5</sup> À publier simultanément avec la présente partie de la CEI 62056.

NOTE Voir aussi la Bibliographie.