

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Electricity metering data exchange – The DLMS/COSEM suite –
Part 8-8: Communication profile for ISO/IEC 14908 series networks**

**Échange des données de comptage de l'électricité – La suite DLMS/COSEM –
Partie 8-8: Profil de communication pour réseaux de la série ISO/IEC 14908**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 IEC, Geneva, Switzerland

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

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

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

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

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Electricity metering data exchange – The DLMS/COSEM suite –
Part 8-8: Communication profile for ISO/IEC 14908 series networks**

**Échange des données de comptage de l'électricité – La suite DLMS/COSEM –
Partie 8-8: Profil de communication pour réseaux de la série ISO/IEC 14908**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 17.220; 35.110; 91.140.50

ISBN 978-2-8322-8082-9

**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
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms, definitions and abbreviated terms	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	12
4 Targeted communication environments.....	13
5 Use of the communication layers for this profile.....	13
5.1 Information related to the use of the standard specifying the lower layers	13
5.2 The structure of the communication profile.....	14
5.3 Lower layers and their use	14
5.3.1 Overview	14
5.3.2 Physical layer	15
5.3.3 Data link layer	15
5.3.4 Network layer	15
5.3.5 Transport layer	15
5.4 Service mapping and Adaptation layer	16
5.4.1 Overview	16
5.4.2 Adaptation layer	16
5.5 Registration and connection management.....	27
6 Identification and addressing schemes	27
7 Specific considerations for the application layer services.....	28
7.1 Overview.....	28
7.2 Application Association establishment and release: ACSE services	28
7.2.1 Application association establishment.....	28
7.2.2 Application association release.....	29
7.2.3 COSEM-OPEN and COSEM-RELEASE service parameters	29
7.3 xDLMS services	30
7.4 Security mechanisms	30
7.4.1 DLMS/COSEM security.....	30
7.4.2 Adaptation layer security	30
7.4.3 Lower layers security	30
7.5 Transferring long application messages	30
7.6 Media access, bandwidth and timing considerations	30
7.7 Other considerations.....	30
8 Communication configuration and management.....	31
9 The COSEM Application Process.....	31
10 Additional considerations for the use of this profile	31
Annex A (informative) Examples	32
Annex B (normative) Interface classes	33
B.1 Interface classes.....	33
B.1.1 ISO/IEC 14908 Identification.....	33
B.1.2 ISO/IEC 14908 Protocol setup	33
B.1.3 ISO/IEC 14908 Protocol status	34

B.1.4	ISO/IEC 14908 Diagnostic	35
B.2	Relation to OBIS	37
Annex C (informative)	Implementation guide and migration path	38
C.1	General.....	38
C.2	Client-server model.....	38
C.2.1	General	38
C.2.2	Clients	38
C.2.3	Servers.....	39
C.2.4	Application associations	39
C.3	The COSEM objects.....	40
C.3.1	COSEM object model.....	40
C.3.2	Referencing methods.....	41
C.3.3	The object_list.....	42
C.3.4	Mandatory COSEM objects.....	42
C.3.5	Application specific objects.....	42
C.3.6	Utility table objects	42
Annex D (informative)	OSGP-AES-128-PSK security suite	46
D.1	General.....	46
D.2	Background.....	47
D.2.1	Overview	47
D.2.2	System Assumptions	47
D.2.3	Threat Model	47
D.2.4	Design goals.....	48
D.2.5	Inspiration	48
D.3	Terms and definition, abbreviated terms and notation	48
D.3.1	Terms and definitions	48
D.3.2	Abbreviated terms	50
D.3.3	Notation.....	50
D.3.4	Other conventions	50
D.4	Cryptographic Primitives	51
D.4.1	General	51
D.4.2	CMAC.....	51
D.4.3	CCM	51
D.5	Cryptographic Functions	52
D.5.1	Overview	52
D.5.2	OSGP_KDF: Key Derivation Function	52
D.5.3	OSGP_MAC: Message Authentication Code Function	52
D.5.4	OSGP_MAC_VERIFY: Message Authentication Code Verification Function	53
D.5.5	OSGP_AE/OSGP_AD: Authenticated Encryption/Decryption Function	53
D.5.6	OSGP_CSPRNG: Cryptographically Secure Pseudo Random Number Generator	55
D.6	Keys	56
D.7	Secure channel initialization	58
D.7.1	Overview	58
D.7.2	Secure Channel State (CryptoContext)	58
D.7.3	Flow	58
D.7.4	Security Suite Negotiation	63
D.7.5	LNAP Commissioning	64

D.7.6	Error Handling and Intrusion Detection	64
D.7.7	Messages	64
D.8	Secure Channel Communication	67
D.8.1	General	67
D.8.2	The General Process	68
D.8.3	Unicast communication	69
D.8.4	Broadcast Communication	73
D.9	Firmware Downloading	75
D.10	Key Management	76
D.10.1	Renewing the Short-term, Meter-unique Keys	76
D.10.2	Renewing the Short-term, Domain-unique Keys	76
D.10.3	UpdateDomainKeysRequest	77
D.10.4	UpdateDomainKeysResponse	77
D.11	Updating the Long-term, Meter-unique Keys	77
D.11.1	General	77
D.11.2	Key Validity Periods	78
D.12	Error Messages	78
D.12.1	Overview	78
D.12.2	AuthenticationFailure	78
D.12.3	SequenceError	78
D.13	Security considerations	78
D.13.1	Reasoning	78
D.13.2	Recommendation and Guidance for Implementers	81
Annex E (normative)	Repeating mechanism	83
E.1	Overview	83
E.2	Terms and definitions	83
E.3	Protocol specification	84
E.3.1	Overview	84
E.3.2	Addressing	84
E.3.3	Service types	84
E.3.4	Timers	84
E.3.5	Request flow	85
E.3.6	Response flow	85
E.3.7	Authentication	85
E.3.8	Examples	86
E.3.9	Broadcast	87
E.4	Downlink frame format	87
E.4.1	Overview	87
E.4.2	Proxy parameters of request frame	88
E.5	Uplink Frame format	92
E.5.1	Overview	92
E.5.2	Proxy success	92
E.5.3	Repeating Failure	93
E.5.4	Authentication failure	93
Annex F (informative)	ISO/IEC 14908-3 Registration and monitoring of LNAPs	94
F.1	Scope	94
F.2	Terms and definitions	94
F.3	Metering device lifecycle	94
F.4	ATM Protocol	94

F.4.1	General	95
F.4.2	ATM roles	95
F.4.3	Automatic discovery	95
F.4.4	Discovery domain	96
F.4.5	ATM messages	96
F.5	Commissioning	100
F.5.1	Overview	100
F.5.2	Commissioning operations	100
Bibliography		101

Figure 1	– Functional reference architecture	13
Figure 2	– Structure of the communication profile	14
Figure 3	– Adaptation layer structure	17
Figure 4	– Unprotected Adaptation layer PDU structure	18
Figure 5	– Protected Adaptation layer PDU structure	19
Figure 6	– Adaptation layer services	20
Figure 7	– Client and server ADP_DATA services	24
Figure D.1	– Key hierarchy diagram	56
Figure D.2	– Secure channel establishment	59
Figure D.3	– Challenge request	60
Figure D.4	– Challenge response	60
Figure D.5	– Commission Request	61
Figure D.6	– Commission response	62
Figure D.7	– Crypto context establishment	67
Figure D.8	– Authenticate encryption mechanism	68
Figure D.9	– Authenticated decryption	69
Figure E.1	– Unacknowledged message exchange	86
Figure E.2	– Request / Response message	86
Figure E.3	– Error during request transmission	86
Figure E.4	– Error during response transmission	87
Figure E.5	– Proxy Repeater proxy message	87
Figure E.6	– Proxy Agent proxy message format	87
Figure E.7	– Proxy Target message format	88
Figure E.8	– Normal ProxyTrailer	90
Figure E.9	– Alternate Key Proxy Trailer	90
Figure E.10	– Proxy SICB field structure	90
Figure E.11	– Alternate Key format	91
Figure E.12	– ProxySubnetNode Address (Type1)	92
Figure E.13	– ProxyUniqueNode_ID Address (Type 2)	92
Figure E.14	– ProxyBroadcast Address (Type 3)	92
Figure E.15	– ProxySubnetNode Compact Address (Type 5 and 7)	92
Figure E.16	– ProxyUniqueNodeCompact Address (Type 6)	92

Table 1	– Control field	118
---------	-----------------------	-----

Table 2 – Client and Server SAP	28
Table 3 – Application associations and data exchange in the DLMS/COSEM over ISO/IEC14908 profile	29
Table C.1 – Pre-established association parameters	40
Table C.2 – base_name range for tables categories	43
Table C.3 – base_names for standard tables BT00 to BT79	44
Table D.1 – Security logical layers	46
Table D.2 – Key type and their scope	57
Table D.3 – Challenge request	65
Table D.4 – Challenge response	65
Table D.5 – Commission request	66
Table D.6 – Commission response structure	67
Table D.7 – Request message	70
Table D.8 – response message structure	70
Table D.9 – Nonce construction	70
Table D.10 – Associated Data construction	71
Table D.11 – Broadcast message	74
Table D.12 – Broadcast nonce	74
Table D.13 – Broadcast Associated Data	74
Table D.14 – Update Domain Keys request	77
Table D.15 – Update Domain Keys response	77
Table D.16 – AuthenticationFailure message	78
Table D.17 – SequenceError message	78
Table D.18 – Example of risks	82
Table E.1 – ProxyHeader format	88
Table E.2 – ProxyDetailedAddress format	89
Table E.3 – ProxyUniformAddress format	89
Table E.4 – ProxyTx control format	89
Table E.5 – Address Type values	90
Table E.6 – Service types	91
Table E.7 – Mode types	91
Table E.8 – Repeating success response	93
Table E.9 – Repeating Failure	93
Table E.10 – Authentication failure code	93
Table F.1 – ATM Message header structure	97
Table F.2 – ATM payloads	97
Table F.3 – ATM-query-ID request structure	98
Table F.4 – ATM-query-ID response structure	98
Table F.5 – ATM-respond-to-query request structure	99
Table F.6 – ATM respond-to-query response structure	99
Table F.7 – Flags	100

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRICITY METERING DATA EXCHANGE –
THE DLMS/COSEM SUITE –****Part 8-8: Communication profile for ISO/IEC 14908 series networks**

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.

International Standard IEC 62056-8-8 has been prepared by IEC technical committee 13, Electrical energy measurement and control.

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

CDV	Report on voting
13/1783/CDV	13/1792/RVC

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

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this 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

The IEC 62056 DLMS/COSEM suite provides specific communication profile standards for communication media relevant for smart metering.

Such communication profile standards specify how the COSEM data model and the DLMS/COSEM application layer can be used on the lower communication media-specific protocol layers.

Communication profile standards refer to communication standards that are part of the IEC 62056 DLMS/COSEM suite or to any other open communication standard.

This International Standard specifies DLMS/COSEM communication profile using ISO/IEC 14908-1:2012, *Information technology – Control network protocol – Part 1: Protocol stack* and ISO/IEC 14908-3:2012, *Information technology – Control network protocol – Part 3: Power line channel specification*. It applies for devices installed on the neighbourhood area network.

It follows the rules defined in IEC 62056-5-3:2017, Annex A, and in IEC 62056-1-0, and IEC TS 62056-1-1 for its structure.

ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE –

Part 8-8: Communication profile for ISO/IEC 14908 series networks

1 Scope

This part of IEC 62056 describes how the DLMS/COSEM Application layer and the COSEM object model as specified in IEC 62056-5-3:2017, IEC 62056-6-1:2017 and IEC 62056-6-2:2017 can be used over the lower layers specified in the IEC 14908 series, forming a DLMS/COSEM ISO/IEC 14908 communication profile.

This document is part of the IEC 62056 series. Its structure follows IEC 62056-1-0 and IEC TS 62056-1-1.

Annex A (informative) provides examples of representative instances of data exchange.

NOTE This Annex A is included and referenced for consistency with other parts of the IEC 62056 suite, but it is empty.

Annex B (normative) defines COSEM interface classes and related OBIS codes for setting up and managing the DLMS/COSEM communication profile for IEC 14908 networks. These interface classes and OBIS codes will be moved later to IEC 62056-6-2 and IEC 62056-6-1.

Annex C (informative) provides an implementation guide and specifies a migration path from Utility Tables based applications to DLMS/COSEM based applications.

Annex D (informative) specifies the OSGP-AES-128-PSK security suite for optional use on the adaptation layer level.

Annex E (normative) specifies the repeating mechanism over the ISO 14908-3 Power Line Channel network.

Annex F (informative) specifies ISO/IEC 14908-3 Registration and monitoring of LNAPs.

2 Normative references

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

IEC 62056-5-3:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer*

IEC 62056-6-1:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-1: Object Identification System (OBIS)*

IEC 62056-6-2:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*

ISO/IEC 14908-1:2012, *Information technology – Control network protocol – Part 1: Protocol stack*

ISO/IEC 14908-3:2012, *Information technology – Control network protocol – Part 3: Power line channel specification*

EN 50065-1, *Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148,5 kHz – Part 1: General requirements, frequency bands and electromagnetic disturbances*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

NOTE All the messages in this document use the big endian format

3.1 Terms and definitions

3.1.1

domain

logical network that is a unit for addressing

Note 1 to entry: Subnet (see below) and node addresses are assigned by the administrator responsible for the domain, and they have meaning only in the context of that domain.

Note 2 to entry: All nodes belongs to the same domain to be able to address each other.

3.1.2

node

abstraction for a physical node that represents the highest degree of address resolvability on a network

Note 1 to entry: A node is identified (addressed) within a subnet by its (logical) node identifier called Node_ID. A physical node may belong to more than one subnet; when it does, it is assigned one (logical) node number for each subnet to which it belongs. A physical node may belong to at most two subnets; these subnets are parts of different domains. A node may also be identified (absolutely) within a network by its Unique_Node_ID which is immutable.

3.1.3

subnet

set of nodes accessible through the same link layer protocol

Note 1 to entry: In a logical address, a subnet is identified by a Subnet_ID.

3.1.4

transaction

sequence of messages that are correlated

Note 1 to entry: For example, a request and the response to the request are all part of a single transaction. A transaction succeeds when all the expected messages from every node involved in the transaction are received at least once. A transaction fails if any of the expected messages within the transaction are not received.

3.2 Abbreviated terms

Abbreviated term	Meaning
AA	Application Association
AARE	Application Association Response
AARQ	Application Association Request
ACSE	Association Control Service Element
ADD	Automated Device Discovery
AdpPDU	Adaptation layer PDU
AL	Application layer
AP	Application Process
APDU	Application Protocol Data Unit
ASE	Application Service Element
ATM	Automated Topology Management
BPSK	Binary Phase Shift Keyed
COSEM	Companion Specification of Energy Metering
CRC	Cyclic Redundancy Code
CSMA	Carrier Sense Medium Access
DC	Data Concentrator
DLPDU	Data Link Protocol Data Unit
DLMS	Device Language Message Specification
FCM	Fast Commission Message
KMS	Key Management System
HES	Head End System
LNAP	Local Network Access Points
MAC	Medium Access Control (sublayer)
MAC	Message Authentication Code (cryptography)
MEP	Multipurpose Expansion Port
NMS	Network Management System
NN	Neighbourhood Network
NNAP	Neighbourhood Network Access Points
OBIS	Object Identification System
OSGP	Open Smart Grid Protocol ^{a)}
OSI	Open System Information
PID	Program Identifier
PLC	Power Line Carrier
PSK	Pre-Shared Key
SAP	Service Access Point
SDU	Service Data Unit
SICB	Service Interface Control Block
UNID	Unique Node Identifier
xDLMS	Extended DLMS
^{a)} OSGP is a business model that defines one method for how smart metering should be implemented, and comprises a variety of items and parameters including security design and implementation, data formats, data model, device functionalities.	

4 Targeted communication environments

The DLMS/COSEM communication profile over IEC 14908 series networks is intended for remote data exchange on Neighbourhood Networks (NN) between Neighbourhood Network Access Points (NNAP) and Local Network Access Points (LNAPs) or metering devices, using BPSK narrowband PLC technology over the low voltage electricity distribution network as a communication medium. The functional reference architecture is shown in Figure 1.

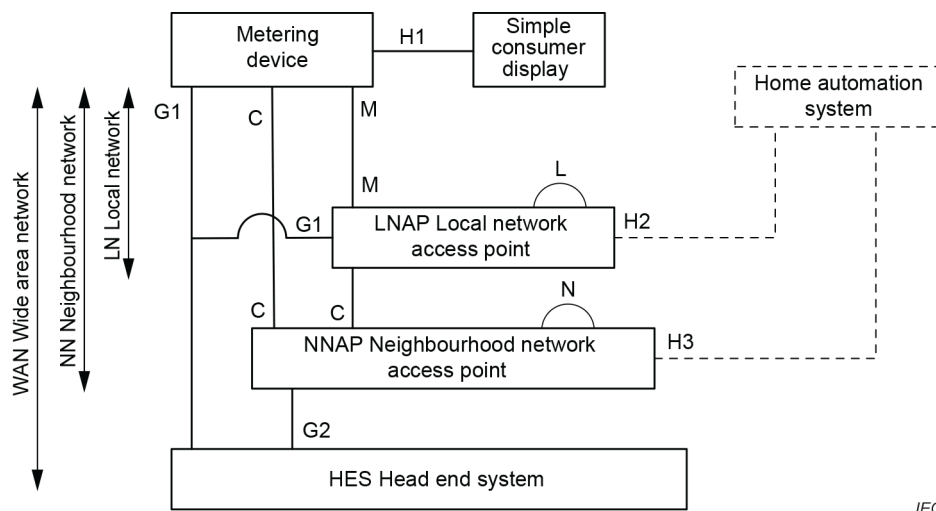


Figure 1 – Functional reference architecture

Metering Devices – typically electricity meters – comprise application functions and communication functions. They may be connected directly to the NNAP via the C interface, or to an LNAP via an M interface, while the LNAP is connected to the NNAP via the C interface. The LNAP function may be co-located with the metering functions.

A NNAP comprises gateway functions and it may comprise concentrator functions. Upstream, it is connected to the Metering Head End System (HES) using suitable communication media and protocols.

Metering Devices and LNAPs may communicate to different NNAPs, but to only one NNAP at a time. From the PLC communication point of view, the NNAP acts as a gateway while metering devices and LNAPs act as endpoints.

NNAPs and similarly LNAPs may communicate with each other, but this is out of the scope of this document, which covers the C interface only.

When the NNAP has concentrator functions, it acts as a DLMS/COSEM client. When the NNAP has gateway functionality only, then the HES plays the role of a DLMS/COSEM client. The metering devices or the LNAPs play the role of DLMS/COSEM servers. In this specification, the NNAP is considered as playing the role of a DLMS/COSEM client, meaning having concentrator functions, therefore, it is also named Data Concentrator (DC).

5 Use of the communication layers for this profile

5.1 Information related to the use of the standard specifying the lower layers

The DLMS/COSEM communication profile over ISO/IEC14908 series networks uses the services of the lower layers specified in ISO/IEC 14908-1:2012 and in ISO/IEC 14908-3:2012.

5.2 The structure of the communication profile

The structure of the DLMS/COSEM communication profile over ISO/IEC 14908 series networks is shown in Figure 2.

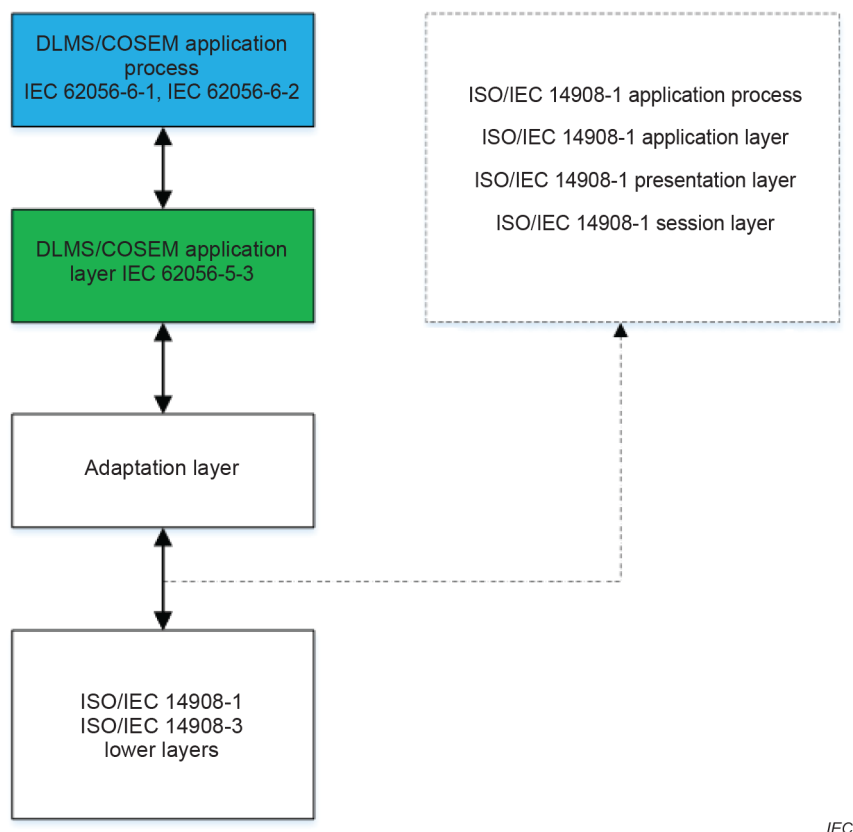


Figure 2 – Structure of the communication profile

The parts shown with solid lines constitute a pure DLMS/COSEM communication profile for ISO/IEC 14908 series networks, using the COSEM data model as specified in IEC 62056-6-1:2017 and IEC 62056-6-2:2017 together with the DLMS/COSEM Application layer as defined in IEC 62056-5-3:2017 and with the lower layers specified in the ISO/IEC 14908 series of standards.

The parts shown with dashed lines are not in the scope of the present document, but are from the ISO/IEC 14908 series of standards.

In the remaining part of this document, all the messages use the big-endian format.

5.3 Lower layers and their use

5.3.1 Overview

The lower layer protocols are specified in ISO/IEC 14908-1:2012 and ISO/IEC 14908-3:2012. They comprise the Physical, the Data link, Network, and Transport layers according to the OSI model.

5.3.2 Physical layer

ISO/IEC 14908-1:2012 allows several types of physical layers. The physical layer used in this standard is for narrowband PLC using BPSK modulation in the CENELEC Frequency Band A. It provides the interface between the equipment and the physical transmission medium, which is the electricity distribution network. It receives and transmits DLPDUs between neighbour nodes by using the PLC technology as defined in ISO/IEC 14908-3:2012, using BPSK modulation in the CENELEC Frequency Band A.

5.3.3 Data link layer

5.3.3.1 Overview

The Data Link layer consists of two parts: the MAC sublayer and the Link layer, as specified in Clauses 6 and 7 of ISO/IEC 14908-1:2012.

5.3.3.2 MAC sublayer

The role of the MAC sublayer is to interface the physical layer and to provide all the necessary mechanisms for the management of the medium in order to liberate the link layer from tasks related to the nature of the medium. This includes predictive p-persistent CSMA algorithm, idle channel detection, the channel backlog estimation and priority slot management. See ISO/IEC 14908-1:2012, 6.1, 6.5 and ISO/IEC 14908-1:2012, Annex A.2.

5.3.3.3 Link layer

The Link layer performs error detection with the means of a CRC. There is no error recovery or acknowledgment available. Corrupted frames are simply discarded. See ISO/IEC 14908-1:2012 Clause 7.

5.3.4 Network layer

The Network layer performs repeating functionality when the network topology is a single channel network topology like bus, token ring, or star topology.

Routing functionality is used when the network topology is a tree or simple topology. A network configuration must be set up first. Addresses used are those configured inside the routers and not those in the PDU exchanged. See ISO/IEC 14908-1:2012, Clause 8.

In the scope of this communication profile the Network layer performs address recognition as specified in ISO/IEC 14908-1:2012, 8.6. It passes inbound packets to the Transport Layer only if the packet is addressed to this node's logical or physical node identifier. Routing is performed by the repeating entity of the Adaptation layer (see Annex E) instead of the Network layer.

This communication profile provides means for application-layer repeating. The layer 3 routing may be disabled if it cannot route as effectively as the repeating algorithm.

5.3.5 Transport layer

5.3.5.1 Overview

The Transport layer consists of the transaction control sublayer and the transport layer itself.

5.3.5.2 Transaction control sublayer

The role of the Transaction control sublayer is to ensure an end-to-end data delivery by providing duplicated packet detection by the receiver, owing to the nature of the network and the possibility for loss of acknowledgment. A transaction consists of a request and a response. A response may contain the requested data, or simply an acknowledgement, or may be absent, at the sender's option. In some situations (like broadcast), a response is not expected. Several mechanisms are available inside the Transaction control sublayer for facilitating detections: identification of the transaction in progress, limitation of the number of concurrent transactions, etc. See ISO/IEC 14908-1:2012, 9.1.

5.3.5.3 Transport layer

The Transport layer controls the end-to-end data transport by verifying that the correct response is received according to the request sent and if not, performs the appropriate retries. See ISO/IEC 14908-1:2012, Clause 10.

5.4 Service mapping and Adaptation layer

5.4.1 Overview

The ISO/IEC 14908-1:2012 protocol stack has, at the top of the Transport layer, the Session, Presentation and Application layers.

In the DLMS/COSEM over ISO/IEC 14908 networks communication profile, an Adaptation layer is located immediately above the Transport layer. The role of the Adaptation layer is to provide the necessary elements for correctly binding the DLMS/COSEM Application layer and the COSEM object model with the lower layers specified in ISO/IEC 14908-1:2012. It also allows the selection of the DLMS/COSEM Application layer and Application process as defined in IEC 62056-5-3:2017 and IEC 62056-6-2:2017.

5.4.2 Adaptation layer

5.4.2.1 General

The Adaptation layer allows the binding of the lower layers with the DLMS/COSEM Application layer.

In addition, it is in charge of the discovery, registration and commissioning processes; see Annex F.

Concerning DLMS/COSEM application layer message exchange, the roles of the Adaptation layer are:

- to provide and manage the path the message shall take for reaching the destination, see 5.4.2.6.2.2.2;
- to redirect the messages to the DLMS/COSEM Application layer depending on the value of the control field during the message reception, see 5.4.2.3.1;
- to provide the required addressing parameters for the client application process and the logical device, see 5.4.2.3.2 items 3 and 4;
- to provide the parameters allowing the correct binding of the higher layer protocol with the Transport layer, see 5.4.2.5;
- to transport the DLMS/COSEM APDUs using the ADP_Data services;
- Security services providing authentication, encryption, and replay prevention are also specified. The main purpose of the Adaptation layer security services is to protect the discovery, registration and commissioning messages. For using Adaptation layer security services to protect the ADP-Data services, refer to 7.4.2.

NOTE These services do not rely on the ISO/IEC 14908-1:2012 session layer security service that provides authentication only.

The Adaptation layer is basically a connectionless protocol. However, a security CryptoContext needs to be established first (see Clause D.7). This CryptoContext establishment is performed during commissioning; see Clause F.5. The CryptoContext may be renewed during the lifetime of the device for example for key updating purposes.

5.4.2.2 Adaptation layer structure

Figure 3 shows the Adaptation layer structure. Although the structure of the Adaptation layer of the NNAP and the LNAP is the same, the content of its elements differs.

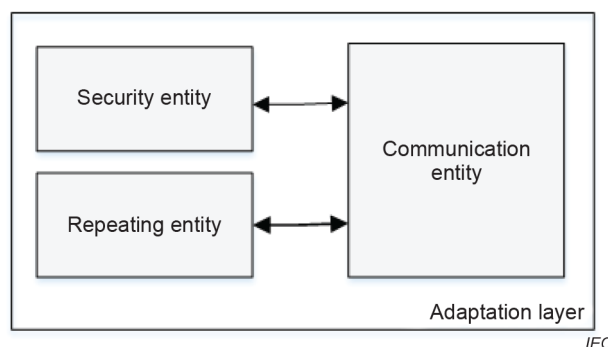


Figure 3 – Adaptation layer structure

The Adaptation layer contains 3 entities:

- a communication entity which is in charge – depending on the configuration of the Adaptation layer – of constructing the PDU for the lower layers during data transmission;
- a security entity which allows the management of the AdpPDU protection, when the Adaptation layer security is activated;
- a repeating entity which allows the indication to the AdpPDU of the path the AdpPDU shall take for reaching the targeted LNAP in the best way.

The communication entity is the same at the NNAP and the LNAP side. It forms, from the service parameters received from the Application layer, the Adaptation layer header during data transmission. During data reception, it processes the Adaptation layer header and presents to the Application layer with the indication primitive, the data received from the other node.

At the NNAP side, a configuration parameter determines if the Adaptation layer security is in force or not. When the Adaptation layer security is in force, a Key Management System (KMS) holds all the symmetric ciphering keys related to all the configured LNAPs inside the network, together with their node identification. It is the scope of the security entity to perform an authenticated encryption of outgoing AdpPDUs ("ciphering") and authenticated decryption and replay prevention of incoming AdpPDUs ("deciphering"). See Annex D for more details.

At the LNAP side, the security entity performs the same functionality as at the NNAP side. The KMS is limited to the Adaptation layer symmetric ciphering key of the related device. The value of the control field received from the NNAP determines if the Adaptation layer security is in force or not.

The repeating entity instructs the message from the NNAP to the LNAP about the best path for reaching the targeted LNAP. The proxy parameters are available in the frames sent by the NNAP only. For more information, refer to Annex E.

5.4.2.3 Adaptation layer PDU structure

5.4.2.3.1 Overview

The Adaptation layer has two kinds of AdpPDUs. An unprotected AdpPDU and a protected AdpPDU, both identified by the Control field as specified in Table 1.

Table 1 shows the possible values the Control field may have and their meaning in the scope of this document.

Table 1 – Control field

Value	Description
0x20	Unprotected AdpPDU
0x21	Protected AdpPDU

The Control field acts as a protocol selector:

- when set to value 0x20, it indicates that the PDU is a DLMS/COSEM Application layer PDU (APDU) with Adaptation layer security not in force;
- when set to value 0x21, it indicates that the PDU is a DLMS/COSEM APDU with Adaptation layer security in force;
- when the value is not 0x20 or 0x21, then the APDU is not a DLMS/COSEM APDU. Refer to ISO/IEC 14908-1:2012, 12.4 in such a case. All the remaining part of this clause is related to DLMS/COSEM over ISO/IEC14908 communication profile.

5.4.2.3.2 NNAP unprotected Adaptation layer PDU structure

The structure of the NNAP unprotected AdpPDU is shown in Figure 4. The AdpPDU contains the header and the payload, and in the downlink parameters, the Proxy parameters are appended:

byte 0								byte n
Proxy parameters				Adaptation layer header				Payload
Proxy Header	Proxy Address(es)	Proxy Cntrl	ProxyTx Trailer	Ctrl Field	Resv	DST SAP	SRC SAP	DLMS APDU

Figure 4 – Unprotected Adaptation layer PDU structure

The proxy parameters contain addressing information required for delivering the message via a series of 1 to 8 repeaters. See Clause E.4.

The NNAP Adaptation layer header consists of the following fields:

- The Ctrl field has a fixed value set to 0x20;
- 'Resv' field is of one byte and is reserved for future. It shall be set to 0;
- 'DST SAP' holds the destination address of the DLMS/COSEM APDU, meaning the logical device SAP when the DLMS/COSEM APDU is from the NNAP to the LNAP and the client SAP when the DLMS/COSEM APDU is from the LNAP to the NNAP. The length of the destination SAP field is of one byte. See Table 2;
- 'SRC SAP' holds the source address of the DLMS/COSEM PDU meaning the client SAP when the DLMS/COSEM PDU is from the NNAP to the LNAP, and the logical device SAP when the DLMS/COSEM PDU is from the LNAP to the NNAP. The length of the source SAP field is of one byte. See Table 2.

The payload is the DLMS/COSEM APDU. It is the remaining part of the AdpPDU that follows the SRC SAP field, up to the end of the message.

5.4.2.3.3 NNAP protected Adaptation layer PDU structure

When the Adaptation layer security is in force, the structure of the NNAP protected AdpPDU is as shown in Figure 5.

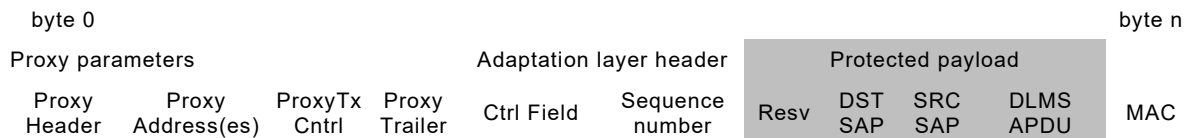


Figure 5 – Protected Adaptation layer PDU structure

where:

- the Ctrl field has a fixed value set to 0x21;
- the Sequence number field is of 4 bytes. It is an increasing value referencing the message. It is reset to 1 every time a new encryption key is derived. It is used for the nonce construction (see Table D.9, and Table D.12) and for the protection against replay attacks; see D.8.4.5;
- the Protected payload, is the encrypted result of the Resv field, the destination SAP, the source SAP and the DLMS/COSEM APDU (see Figure 4), concatenated in this order. These fields are encrypted and authenticated using the algorithms as described in Clause D.4. For more information see Annex D;
- the message authentication code (MAC). The length of the MAC is 8 bytes. The MAC is related to the Protected payload. For more information, refer to Annex D.

5.4.2.3.4 LNAP Adaptation layer structure

When the frame is from the LNAP to the NNAP, the AdpPDU structure is the same as the one specified in 5.4.2.3.2 and 5.4.2.3.3, except that the Proxy parameters are not present.

5.4.2.4 Adaptation layer maximum data length

The maximum length of the AdpPDU is limited to 228 bytes.

When protection is not in force, this length includes:

- the Proxy parameters, which may be up to 48 bytes (a maximum of 8 repeaters is allowed);
- the Adaptation layer header;
- the payload i.e. the DLMS/COSEM APDU.

When the Adaptation layer protection is in force, it includes also the lengths of the Sequence number parameter and the MAC.

5.4.2.5 Adaptation layer services

5.4.2.5.1 Service mapping

The role of the Adaptation layer is to redirect the APDU to the DLMS/COSEM Application layer depending on the value of the control field (see Table 1), and to provide the necessary procedures and services for binding the lower layers to the Application layer. Figure 6 presents the services offered by the Adaptation layer.

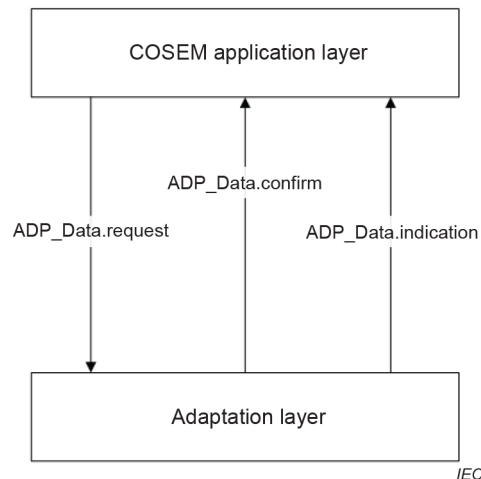


Figure 6 – Adaptation layer services

5.4.2.5.2 Service specification

5.4.2.5.2.1 General

As the protocol of the Adaptation layer is connectionless protocol, it provides only ADP_Data services: ADP_Data.request, ADP_Data.confirm and ADP_Data.indication.

5.4.2.5.2.2 ADP_Data.request

Function

The ADP_Data.request primitive is invoked by the DLMS/COSEM Application layer to the Adaptation layer to request sending an Adaptation layer PDU to the peer Adaptation layer entity using the transmission procedures.

Semantics

The semantic of the primitive is as follows:

```

ADP_Data.request
(
    service_type,
    device_address,
    destination_SAP,
    source_SAP,
    Data
)
    
```

where:

The service_type parameter specifies which TPDU type should be used for transporting the Data. The service_type parameter is mapped from the Invoke-Id-And-Priority service class field of the xDLMS services or the response-allowed parameter of the InitiateRequest APDU:

- when the service_class field of the Invoke-Id-And-Priority parameter is of type confirmed or the response-allowed parameter or the InitiateRequest APDU is TRUE, then the service_type should be of type confirm;
- when the service_class field of the Invoke-Id-And-Priority parameter is of type unconfirmed or the response-allowed parameter of the InitiateRequest APDU is FALSE, then the service_type should be of type unconfirm.

Table 3 specifies the mapping of the service-class field of the Invoke-Id-And-Priority and response-allowed parameters into the service_type parameter.

The device_address parameter contains the destination ISO/IEC 14908 address of the device the data has to be delivered to. It is made up of the subnet_ID and the node_ID. The domain_ID is a configuration parameter populated in the NNAP during commissioning.

The destination_SAP parameter specifies the address of the remote SAP involved in the Data transmission.

The source_SAP parameter specifies the address of the SAP where the service is requested from.

The Data parameter specifies the PDU to be transferred using the Adaptation layer services.

Use

This primitive is used by the DLMS/COSEM Application layer when it has Data to send to the destination Application layer.

When the Adaptation layer receives this primitive, it will construct the AdpPDU to make available for the lower layers by inserting the Control field, the reserved field, the destination_SAP and the source_SAP at the beginning as specified in Figure 4, and if the protection is in force, then applies the protection (see Figure 5).

If the sender is the NNAP, then the proxy parameters are also inserted. See Annex E for the construction of the proxy parameters.

Once this process is done, the Adaptation layer invokes the lower layer data transmission primitive.

5.4.2.5.2.3 ADP_Data.confirm

Function

The ADP_Data.confirm primitive issues a local confirmation upon the completion of the Data transmission to the lower layer, at the Adaptation layer level. The scope of this primitive is only local. It notifies the Application layer – having invoked an ADP_Data.request primitive – of the result of the processing of the related request. This result may be SUCCESS or FAILED.

Semantics

The semantic of the primitive is as follows:

```
ADP_Data.confirm
(
    device_address,
    destination_SAP,
    source_SAP,
    status
)
```

The device_address parameter contains the destination ISO/IEC 14908 address of the device the data is delivered to. The value of this parameter is the same as the one provided in the corresponding ADP_Data.request primitive.

The `destination_SAP` parameter specifies the address of the remote SAP involved in the data transmission. The value of this parameter is the same as the one provided in the corresponding `ADP_Data.request` primitive.

The `source_SAP` parameter specifies the address of the SAP where the service is requested from. The value of this parameter is the same as the one provided in the corresponding `ADP_Data.request` primitive.

The status parameter is used for providing a local result (SUCCESS or FAILED) of the data transmission related to the `ADP_Data.request` previously issued.

Use

This primitive is locally generated by the Adaptation layer to the local Application layer entity as a response to an `ADP_Data.request` primitive to inform the originator of the request about the result of the data transmission procedures.

5.4.2.5.2.4 ADP_Data.indication

Function

The `ADP_Data.indication` primitive is passed from the Adaptation layer entity to the Application layer entity for notifying it about the arrival of an `AdpPDU` from the peer station or an error from the Transport layer. This primitive defines the transfer of Data from the Adaptation layer entity to the Application layer entity.

Semantics

The semantic of the primitive is as follows:

```
ADP_Data.indication
(
    service_type,
    source_address,
    destination_SAP,
    source_SAP,
    status,
    Data
)
```

The `service_type` is a parameter indicating the type of service: whether it is confirm or unconfirm service type.

The `source_address` parameter is the ISO/IEC 14908 physical address of remote device the Data is originated from. The `source_address` parameter is provided to the Adaptation layer by the Transport layer. See ISO/IEC 14908-1:2012, 8.3, `Rcv_Packet(address_pair, pduType, PDU, priority)` primitive.

The `destination_SAP` parameter specifies the address of the logical device SAP when the DLMS/COSEM APDU is from the NNAP to the LNAP, and the `client_ID` when the DLMS/COSEM APDU is from the LNAP to the NNAP. The `destination_SAP` parameter is part of the Adaptation layer header as provided by the remote device. See 5.4.2.3.2.

The `source_SAP` parameter specifies the address of the SAP of the application process that sent the DLMS/COSEM APDU. The `source_SAP` parameter is part of the Adaptation layer header as provided by the remote device. See 5.4.2.3.2.

The status parameter informs the Application layer about the arrival of Data. In case of failure, the status parameter provides an error code and the Data parameter is simply empty. See Clause D.12.

The Data parameter carries the DLMS/COSEM APDU received using the Adaptation layer service. See 5.4.2.3.2.

Use

The ADP_Data.indication primitive is passed from the Adaptation layer entity to the Application layer entity for informing the Application layer entity about the arrival of Data from a remote Adaptation layer user entity. NNAP requests are notified to the LNAP by a ADP_Data.indication primitive at the LNAP Application layer level. In turn, LNAP responses to NNAP requests are notified to the NNAP by an indication at the NNAP Application layer level.

5.4.2.6 Protocol specification

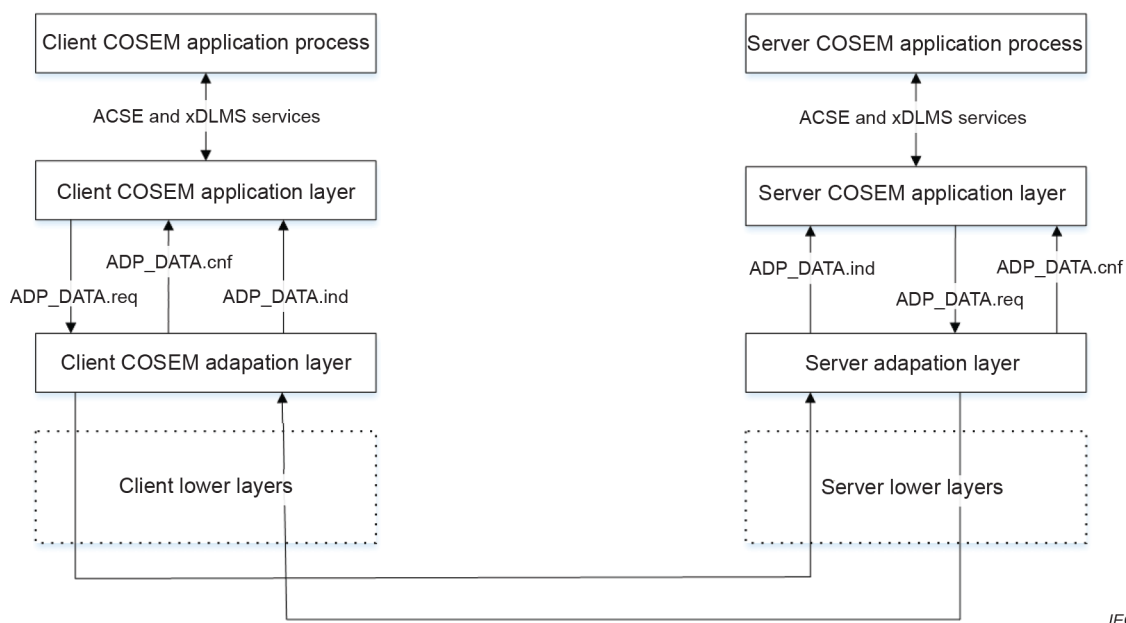
5.4.2.6.1 Overview

The data exchange is based on *client-server* paradigm. The client sends a request to the server and then – if the request is of type confirmed – the server responds to this request as shown in Figure 7.

Data transmission is initiated upon the initiative of the DLMS/COSEM client Application layer when this entity has a request to send. When the DLMS/COSEM client Application layer invokes the ADP_Data.request, it provides with the request the physical device destination address, the client SAP and the server SAP. The Adaptation layer processes this request and invokes the Transport layer services for transmission.

At the LNAP side, the server Adaptation layer receives the data from its Transport layer and processes it in order to provide the relevant ADP_Data.indication to its Application layer. This indication carries the request as sent by the client to which the server Application layer has to respond, depending on the indication service type. The response, if any, is provided by the Application layer with the means of an ADP_Data.request primitive to its Adaptation layer, which has to process it and make it available to the Transport layer for transmission.

At the NNAP side, the client Adaptation layer receives the data from its Transport layer and processes it in order to provide the relevant ADP_Data.indication to its Application layer. This indication carries the response as sent by the server to its request.



IEC

Figure 7 – Client and server ADP_DATA services

5.4.2.6.2 Request management

5.4.2.6.2.1 General

Any confirmed request received at the Adaptation layer level needs to be responded to (meaning that an ADP_Data.indication has to be invoked by the Adaptation layer) before the next ADP_Data.request can be invoked by the Application layer. Cancellation is provided by the Transport layer when its transaction fails. See 5.3.5.2. Any new request received from the Application layer, before the response to the previous one is received, is simply discarded.

5.4.2.6.2.2 Sending data – NNAP side

5.4.2.6.2.2.1 Adaptation layer header

The NNAP Adaptation layer maintains, as specified in 5.4.2.2, a configuration parameter which indicates if protection is in force or not. When the protection is in force, it concerns all the nodes available in the subnetwork. In this case, a KMS (Key Management System) is available in the NNAP. It holds all the security keys related to each node of the subnetwork.

When the NNAP Adaptation layer is requested to transmit data to a given L NAP, it first inserts the relevant Control field depending on whether the protection is force or not.

After that, it inserts the reserved field, the destination SAP, the source SAP followed by the Application layer APDU as provided by the Application layer.

If the protection is not in force, then the message that is built is passed to the repeating entity for the inclusion of the proxy parameters. The AdpPDU as constructed is made available for the Transport layer, using the appropriate primitive.

When the protection is in force, the Adaptation layer constructs the AdpPDU by inserting the relevant Control field, and then the reserved field, the destination SAP, the source SAP, followed by the APDU as provided by the Application layer. After this, the Adaptation layer requests the protection of the message to be built by the security entity. This protection consists of the encryption then the MAC calculation of the part of the message, starting with the reserved field followed by the destination and the source SAPs, and the DLMS/COSEM APDU provided by the DLMS/COSEM Application layer, using the symmetric key shared by the NNAP and the relevant L NAP. Once this operation is performed, the Adaptation layer security entity:

- inserts the four-bytes request sequence number immediately after the Control field;
- inserts the encrypted message that is constructed;
- and then, adds the calculated MAC after the protected payload, see Figure 5.

The message that is built is passed to the repeating entity for the inclusion of the proxy parameters. The AdpPDU as constructed is made available to the Transport layer, using the appropriate primitive.

5.4.2.6.2.2.2 Proxy parameters

The exchanges are based on the master/slave principle where the slaves (the LNAPs) are only allowed to transmit upon the invitation of the NNAP. A typical network is controlled by the NNAP, which also plays the role of the network topology manager. All LNAPs have repeating capability. To extend the communication range, the Repeating entity of the NNAP Adaptation layer may instruct the LNAPs inside the communication network about the best path the Application message should take to reach the destination. This path is specified in the Proxy parameters carried by the AdpPDU. The message is then transferred from hop to hop, up to the final destination. For more details, refer to Annex E.

Internally, the Repeating entity of NNAP Adaptation layer manages a repeating table that allows it to have knowledge of the order of the repeater LNAPs needed, hop by hop, for reaching each destination (see E.2.3) available in the subnetwork. For a given destination device address, the Repeating entity of the NNAP Adaptation layer extracts LNAP addresses from the repeating table for repeaters, and then builds the Proxy parameters field of the AdpPDU. The Proxy parameters are as specified in Figure 4 and Figure 5, meaning that the Proxy Header, the Proxy Addresses, the Proxy Control and Proxy Trailer fields are inserted at the beginning of the frame as specified in Clause E.3.

5.4.2.6.2.2.3 Lower layer service invocation

Once the operations specified in 5.4.2.6.2.2.2 are completed, the Adaptation layer makes the message available to the Transport layer with the appropriate service_type in the service primitive; see ISO/IEC 14908-1:2012, 10.4:

- when the service_type parameter is of type confirm, then the TPDU type to use should be request/response;
- when the service_type parameter is of type unconfirm, then the TPDU type to use should be Unackd-Rpt.

5.4.2.6.2.2.4 Transport layer confirmation

After making available the message to the Transport layer for transmission, the Adaptation layer then builds and sends a successful ADP_Data.confirm primitive to the Application layer whenever the AdpPDU has been successfully provided to the Transport layer. Otherwise, the Transport layer communicates a failure to the Adaptation layer.

5.4.2.6.2.3 Sending data – Server side

5.4.2.6.2.3.1 Adaptation layer header

The LNAP always sends a response to a confirmed request coming from the NNAP after the LNAP Application layer issues an ADP_Data.request primitive with a confirm service type (a LNAP can never send an unconfirm request). Applying the protection is specified by the control field:

- a) if the Control field of the request received from the NNAP is equal to Protected AdpPDU (value 0x21, see Table 1), then the response to be sent by the LNAP shall be a protected payload;

- b) if the Control field of the request received from the NNAP is an Unprotected AdpPDU (value 0x20, see Table 1), then the response to be sent by the LNAP shall be a non-protected payload.

When the LNAP Adaptation layer is requested to transmit data to the NNAP, it simply copies the Control field received from the NNAP into the response, adds the reserved field, and then fills the destination and source SAP fields, followed by the Application layer PDU.

If the protection is not in force, the Adaptation layer makes the message available to the Transport layer, because the Proxy parameters are not needed for AdpPDUs from the LNAP to the NNAP. The source and destination SAPs are provided in the ADP_Data.request originated by the Application layer.

When the security is in force, the LNAP Adaptation layer communication entity performs the sequence described above for the non-protected payload, then passes the data to the security entity, which performs the protection by making use of the security material available. Each server stores, at the Adaptation layer level, all the security parameters needed for the Adaptation layer payload protection. These security parameters are:

- the unicast encryption key (UCK) and the broadcast encryption key (BCK), which are obtained via key derivation, see Clause D.6;
- the unicast request and receive sequence numbers and the receive broadcast sequence number, which are of 4 bytes each. See D.8.3.3 and D.8.4.3;
- the meter unique identifier and the domain-ID for the nonce calculation.

The protection consists of the encryption and the MAC calculation for the part of the message, made up of the reserved field, the destination and source SAPs and the DLMS/COSEM APDU.

The Adaptation layer communication entity then concatenates to the Control field the transmit Sequence number, the protected payload as prepared by the security entity, and then the MAC. Then it makes the message available to the Transport layer.

5.4.2.6.2.3.2 Proxy parameters

There are no proxy parameters when the response message is transmitted from the LNAP to the NNAP.

5.4.2.6.2.3.3 Lower layer service invocation

At the LNAP side, the Adaptation layer communication entity does not process the service_type field. An ADP_Data.request sent by the LNAP Adaptation layer is always of confirm type.

5.4.2.6.2.3.4 Transport layer confirmation

After making available the data to the Transport layer for transmission, the Adaptation layer communication entity builds and sends a successful ADP_Data.confirm to the Application layer whenever the AdpPDU is successfully provided to the lower layer. Otherwise, the Transport layer communicates a failure to the Adaptation layer communication entity. See ISO/IEC 14908-1:2012, 11.3.

5.4.2.6.3 Receiving data – NNAP side

5.4.2.6.3.1 Proxy parameters management

The AdpPDU from the LNAP to the NNAP never carries Proxy parameters.

5.4.2.6.3.2 Adaptation layer header

During reception, the Adaptation layer receiving entity begins with the analysis of the Control field:

- a) if the Control field is equal to Unprotected AdpPDU (value = 0x20), then the communication entity of the Adaptation layer extracts the destination and source SAP and the APDU from the AdpPDU received, and then builds the ADP_Data.indication primitive for the Application layer;
- b) if the Control field is equal to Protected AdpPDU (value = 0x21), then the Adaptation layer communication entity passes the data to the security entity, which verifies and removes the protection. The protection verification consists of:
 - checking the received sequence number carried by the message, which has to be greater than the last sequence number stored in the NNAP security entity for the related LNAP;
 - the deciphering and the verification of the MAC using the security material available in the configuration parameters for the related LNAP.

When the protection verification is successful, the Adaptation layer communication entity uses the destination and source SAPs and the APDU carried by the frame, to invoke the ADP_Data.indication primitive in order to notify the Application layer of the availability of the data received.

When the protection verification of the request message fails, then the data is simply discarded and the Adaptation layer forms and sends an error response to the Application layer with the indication primitive. In such a case, the Data field is simply void. See Clause D.12.

5.4.2.6.4 Receiving data – LNAP side

5.4.2.6.4.1 Proxy parameters management

At each hop, once a given LNAP Repeater notices that it is not the final destination of the frame, it consumes its own address in the frame and redirects the remaining part of the frame to the next hop, and so on, until the frame reaches the destination. For more information, see Annex E.

5.4.2.6.4.2 Adaptation layer header

The protocol for receiving is the same at the NNAP and the LNAP Adaptation layer.

5.4.2.7 Segmentation and reassembly

Segmentation is not supported. See also 7.5.

5.5 Registration and connection management

The registration and connection management is specified in Annex F.

6 Identification and addressing schemes

During the registration process, an LNAP obtains from the NNAP a physical device address which is made up of the domain_ID, the subnet_ID and the node_ID. In the scope of this specification, the size of the domain_ID shall be of 3 bytes. See ISO/IEC 14908-1:2012, Clauses E.1, E.2 and E.6.

The physical device source and destination addresses are transported within every frame using the MAC sublayer services.

At the top of the protocol stack on the NNAP side, the client Application Process uses the client SAP for its addressing. Several client Application Processes may be located inside the same physical entity. Each of them is identified by its SAP.

At the top of the protocol stack at the LNAP side, several logical devices may be located inside the same physical device. Each logical device can be reached at its SAP.

An Application Association established between a specific client and a specific logical device is identified by the {(Client Physical device address, Client ID), (Server Physical device address, Server logical device ID)} doublet.

Table 2 provides the SAPs for the client and the server.

Table 2 – Client and Server SAP

Client SAPs	
No-station	0x00
Client Management Process	0x01
Public Client	0x10
Open for client SAP assignment	0x02... 0x0F and 0x11 to FF
Server SAPs	
No station	0x00
Management Logical Device	0x01
Reserved for future use	0x02... 0x0F
Open for server SAP assignment	0x10...0x7E
All-station (Broadcast)	0xFF

7 Specific considerations for the application layer services

7.1 Overview

The present clause defines the specific constraints for using the DLMS/COSEM application layer in this communication profile.

7.2 Application Association establishment and release: ACSE services

7.2.1 Application association establishment

To be able to establish an AA between the LNAP and the NNAP managing the subnetwork, the LNAP has to be discovered and configured first.

As specified in IEC 62056-5-3:2017, AAs may be explicitly established or preestablished. To explicitly establish AAs, the client uses the ACSE services. No specific constraints apply.

Both explicitly established and preestablished AAs may be confirmed or unconfirmed.

Table 3 shows the rules for explicitly establishing confirmed and unconfirmed AAs, the type of data transfer services available in such AAs and the AdpPDU types used for carrying APDUs. In this table, grey areas represent cases which are out of the normal operating conditions: either not allowed or have no useful purpose.

**Table 3 – Application associations and data exchange
in the DLMS/COSEM over ISO/IEC14908 profile**

Application association establishment				Data exchange	
Protocol connection parameters	COSEM-OPEN service class	Use	Type of established AA	Service class	ADP-Data service type
Phy device address: {domain ID, subnet_ID, node_ID}	Confirmed	AARQ/AARE using ADP-Data services	Confirmed	Confirmed data exchange allowed	ADP-Data confirm
				Unconfirmed data exchange allowed	ADP-Data unconfirm
	Unconfirmed		Unconfirmed	Confirmed data exchange not allowed	-
				Unconfirmed data exchange allowed	ADP-Data unconfirm

Data exchange using confirmed and/or unconfirmed services may take place in a confirmed AA.

Data exchange using a confirmed service cannot take place in an unconfirmed AA.

7.2.2 Application association release

The layer (N-1) of the Application layer, meaning the Adaptation layer in this profile, has a connectionless oriented protocol. Therefore, the AA can only be closed with the means of the ACSE A-RELEASE services – by invoking the COSEM-RELEASE.request primitive.

7.2.3 COSEM-OPEN and COSEM-RELEASE service parameters

The service parameters of the COSEM-OPEN service shall be used as described below:

The Protocol_Connection_Parameters parameters shall be:

Protocol (Profile) Identifier	ISO/IEC 14908
Server_subnet_ID	Subnetwork to which the device belongs ¹⁾
Server_node_ID	Node identifier assigned to the device during the registration
Server_SAP	COSEM Logical Device Address SAP
Client_subnet_ID,	Subnetwork to which the client belongs ¹⁾
Client_node_ID	Node Identifier assigned to the client
Client_SAP	COSEM client application process (type) identifier

¹⁾ See E.3.2.

The User_information parameter service is not used.

The service_class parameter is specified in Table 3.

The Use_RLRQ_RLRE parameter of the COSEM-RELEASE.request primitive shall be set to TRUE. The User_information parameter service is not used.

7.3 xDLMS services

The communication profile specified in this document allows the use of all xDLMS services specified in IEC 62056-5-3:2017 standard within an application context using LN referencing or SN referencing except that – due to the transaction principle of the lower layers – unsolicited services cannot be used.

7.4 Security mechanisms

7.4.1 DLMS/COSEM security

The DLMS/COSEM security mechanisms specified in IEC 62056-5-3:2017 and in IEC 62056-6-2:2017 apply at the application layer and the application process level. They can be used without any restriction.

7.4.2 Adaptation layer security

7.4.2.1 Introduction

Applying adaptation layer security to ADP_Data messages are controlled by the Control field of those messages, see 5.4.2.3.1.

7.4.2.2 Security suite

7.4.2.2.1 Overview

This document supports OSGP-AES-128-PSK security suite as specified in D.2.5.

7.4.2.2.2 OSGP-AES-128-PSK

The OSGP-AES-128-PSK (see IETF RFC 5433) security suite provides a secure, mutually authenticated, two-way communication channel between a NNAP and a LNAP. The secure channel provides data confidentiality, integrity, authentication and replay protection.

7.4.3 Lower layers security

In addition to the DLMS/COSEM security and the Adaptation layer security, the lower layers may present security. These security features are out of the scope of this document.

7.5 Transferring long application messages

Transferring long application messages is achieved with the means of the DLMS/COSEM General Block Transfer mechanism that supports confirmed transfer with streaming and block recovery as well as unconfirmed transfer with streaming. This mechanism may convey any large message.

xDLMS service specific block transfer may also be used in the scope of point to point communication.

7.6 Media access, bandwidth and timing considerations

At the Application process and Application layer levels, there are no specific considerations. All the timing and bandwidth constraints are managed at the Transport and Physical layer level.

7.7 Other considerations

Void.

8 Communication configuration and management

The communication configuration parameters are managed with the means of the DLMS/COSEM IEC 14908 interface classes as specified in Annex B. Annex F specifies the Registration and Connection management.

9 The COSEM Application Process

All the features, as defined in the IEC 62056-6-1:2017, IEC 62056-6-2:2017 and IEC 62056-5-3:2017, using the request/response paradigm may be used without any restriction.

See also Annex C that defines a migration path from applications using Utility Tables to full COSEM based applications.

10 Additional considerations for the use of this profile

Void.

Annex A (informative)

Examples

Void.

Annex B (normative)

Interface classes

B.1 Interface classes

B.1.1 ISO/IEC 14908 Identification

Instances of the ISO/IEC 14908 Identification interface class allow the identification of the device and the network to which the device is connected to.

ISO/IEC14908 Identification		0...n				class_id = 130, version = 0			
Attributes		Data type		Min.	Max.	Def.	Short name		
1.	logical_name (static)	octet-string					x		
2.	node_Id (static)	unsigned		1	127		x + 0x08		
3.	subnet_ID (static)	unsigned		1	255		x + 0x10		
4.	domain_ID (static)	octet-string					x + 0x18		
5.	program_ID (static)	octet-string					x + 0x20		
6.	unique_node_ID (static)	octet-string					x + 0x28		
Specific methods		m/o							

Attribute description

logical_name	Identifies the "ISO/IEC 14908 Identification" object instance. See Clause B.2.
node_ID	Identification of the node.
subnet_ID	Identification of the subnet to which the device is connected to.
domain_ID	Identification of the network. It shall be 3 bytes.
program_ID	Uniquely identifies the functionalities and version of the firmware running on the device. It shall be 8 bytes.
unique_node_ID	Identification of the physical connection module connected to the ISO/IEC 14908-1:2012 network. Each compliant module is assigned a unique 48-bit identifier called Unique_Node_ID. This ID is unique worldwide and is set at the time of manufacture. The value of this identifier does not change from the time of manufacture.

B.1.2 ISO/IEC 14908 Protocol setup

Instances of the ISO/IEC 14908 Protocol setup interface class allow the configuration of the ISO/IEC 14908 device.

ISO/IEC 14908 Protocol setup	0...n	class_id = 131, version = 0			
Attributes	Data type	Min.	Max.	Def.	Short name
1. logical_name (static)	octet-string				x
2. inactivity_timeout (static)	long-unsigned				x + 0x08
Specific methods	m/o				

Attribute description

logical_name	Identifies the "ISO/IEC 14908 Protocol setup" object instance. See Clause B.2.
inactivity_timeout	Minutes of absence of Adaptation layer messages from the NNAP before the LNAP is considered to be out of communication; see F.4.3.

B.1.3 ISO/IEC 14908 Protocol status

Instances of the ISO/IEC 14908 Protocol status interface class allow having knowledge about the status of the protocol in the ISO/IEC 14908 device.

ISO/IEC 14908 Protocol status	0...n	class_id = 132, version = 0			
Attributes	Data type	Min.	Max.	Def.	Short name
1. logical_name (static)	octet-string				x
2. transmission_errors (dyn)	long-unsigned				x + 0x08
3. transmit_tx_failure (dyn)	long-unsigned				x + 0x10
4. transmit_tx_retries (dyn)	long-unsigned				x + 0x18
5. receive_tx_full (dyn)	long-unsigned				x + 0x20
6. lost_messages (dyn)	long-unsigned				x + 0x28
7. missed_messages (dyn)	long-unsigned				x + 0x30
8. layer2_received (dyn)	long-unsigned				x + 0x38
9. layer3_received (dyn)	long-unsigned				x + 0x40
10. messages_received (dyn)	double-long-unsigned				x + 0x48
11. messages_validated (dyn)	double-long-unsigned				x + 0x50
Specific methods	m/o				

Attribute description

logical_name	Identifies the "ISO/IEC 14908 Protocol status" object instance. See Clause B.2.
transmission_errors	This is a count of the number of transmission errors that have occurred on the network. A transmission error is detected via a CRC error during packet reception or as a packet that is less than 8 bytes long. This could result from a collision, a noisy medium, signal attenuation, etc. See ISO/IEC 14908-1:2012, 13.8.2.
transmit_tx_failure	The number of times that the node failed to receive expected acknowledgments or responses after retrying the configured number of times. See ISO/IEC 14908-1:2012, Clause B.8.

transmit_tx_retries	The number of retries sent by this node. This does not include retries used for messages sent with repeated service. See ISO/IEC 14908-1:2012, Clause B.8.
receive_tx_full	The number of times that an incoming packet was discarded because there was no room in the transaction database. See ISO/IEC 14908-1:2012, Clause B.8.
lost_messages	This is the number of messages that were addressed to the node that were thrown away because there was no application buffer available for the message. See ISO/IEC 14908-1:2012, 13.8.2.
missed_messages	This is the number of messages that were on the network but could not be received because there was no network buffer (packet buffer) available for the message or the network buffer was too small to receive the message. See ISO/IEC 14908-1:2012, 13.8.2.
layer2_received	The number of Layer-2 messages received by this node. Layer-2 messages are those that have correct CRC and can be addressed to any node. See ISO/IEC 14908-1:2012, B.8.
layer3_received	The number of messages transmitted from layer 3 of the protocol processor. These can include network variable updates, explicit messages, acknowledgments, retries, reminders, service pin messages, and any other type of message. See ISO/IEC 14908-1:2012, Clause B.8.
messages_received	Number of messages received, which are delivered to the Adaptation layer.
messages_validated	Number of correct messages received at Adaptation layer level.

B.1.4 ISO/IEC 14908 Diagnostic

Instances of the ISO/IEC 14908 Diagnostic interface class allow to have knowledge about the device status inside the PLC network.

ISO/IEC 14908 Diagnostic		0...n	class_id = 133, version = 0			
Attributes		Data type	Min.	Max.	Def.	Short name
1.	logical_name (static)	octet-string				x
2.	plc_signal_quality_status (dyn)	enum				x + 0x08
3.	com_module_state (dyn)	enum				x + 0x10
4.	received_message_status (dyn)	unsigned				x + 0x18
5.	no_receive_buffer (dyn)	long-unsigned				x + 0x20
6.	transmit_no_data (dyn)	long-unsigned				x + 0x28
7.	backlog_overflows (dyn)	long-unsigned				x + 0x30
8.	late_ack (dyn)	long-unsigned				x + 0x38
9.	frequency_invalid (dyn)	long-unsigned				x + 0x40
Specific methods		m/o				

Attribute description	
logical_name	Identifies the "ISO/IEC 14908 Diagnostic" object instance. See Clause B.2.
plc_signal_quality_status	Provide the PLC signal quality status: enum (0) No PLC traffic detected, (1) PLC traffic detected, but no traffic addressed to this device, (2) A packet addressed to this device has been received. The signal margin is less than or equal to 9 dB, (3) A packet addressed to this device has been received. The signal margin is between 12 dB or 15 dB, (4) A packet addressed to this device has been received. The signal margin is greater than or equal to 18 dB, (5) Meter is commissioned but its inactivity_timeout as defined in B.1.2. has expired. The last packet addressed to this meter had a signal margin is less than or equal to 9 dB, (6) Meter is commissioned but its inactivity_timeout as defined in B.1.2. has expired. The last packet addressed to this meter had a signal margin at 12 dB or 15 dB, (7) Meter is commissioned but its inactivity_timeout as defined in B.1.2. has expired. The last packet addressed to this meter had a signal margin greater than or equal to 18 dB This parameter is updated every time a packet is received by the device.
com_module_state	Last received state of the device's power line ISO/IEC 14908 communication module: (0, 1) Invalid states, (2) Unconfigured, (3) Applicationless, (4) Configured, (6) Hard-offline, (12) Configured, soft offline, (140) Configured, in bypass mode, (255) No reply when status requested This field is updated on each device power-up, each re-synch request from the NNAP, and each communication module reset. Any value which is not listed above is invalid state. See ISO/IEC 14908-1:2012, 13.4, and 13.8.4

received_message_status	Status of the received message: b0: PLC Link Explicit Message Received, b1: reserved, b2: reserved, b3: reserved, b4: reserved, b5 – b7: Transceiver phase 0: No phase inversion present, 1: In Phase normal, 2: Plus 120 degrees inverted, 3: Minus 120 degrees normal, 4: Phase 180 degrees inverted, 5: Plus 120 degrees normal, 6: Minus 120 degrees inverted, 7: N.A
no_receive_buffer	Number of times the ISO/IEC 14908-1:2012 lower layers detected a network inbound packet addressed to it, but has no buffer to store it. Hence the message could not be made available to the Adaption layer.
transmit_no_data	Number of times the Adaptation layer attempted to transmit data to the ISO/IEC 14908-1:2012 stack but no buffer is available. Updated on occurrence. ISO/IEC 14908-1:2012, 13.4.
backlog_overflows	Number of times the MAC layer predictive backlog counter overflowed. See ISO/IEC 14908-1:2012, Clause B.8.
late_ack	Number of times an ACK or response was received for a transaction that has been already completed. Typically, this occurs owing to too short transaction timer values or network congestion.
frequency_invalid	Number of times the ISO/IEC 14908-1:2012 stack detects an invalid frequency. Updated on occurrence.

B.2 Relation to OBIS

For setting up and managing data exchange using ISO/IEC 14908 PLC networks at least one instance of each of the following interface classes shall be implemented:

	IC	OBIS identification					
		A	B	C	D	E	F
ISO/IEC 14908 Identification	130, ISO/IEC 14908 Identification	0	<i>b</i>	32	0	0	255
ISO/IEC 14908 Protocol setup	131, ISO/IEC 14908 Protocol setup	0	<i>b</i>	32	1	0	255
ISO/IEC 14908 Protocol status	132, ISO/IEC 14908 Protocol status	0	<i>b</i>	32	2	0	255
ISO/IEC 14908 Diagnostic	133, ISO/IEC 14908 Diagnostic	0	<i>b</i>	32	3	0	255

Annex C (informative)

Implementation guide and migration path

C.1 General

The purpose of this informative Annex is to facilitate implementation of the communication profile specified in this document by recapitulating some basic principles of DLMS/COSEM specified in IEC 62056-5-3:2017 and in IEC 62056-6-2:2017 and showing a migration path from ANSI Utility table based applications to COSEM object-based applications, via the COSEM "Utility tables" objects.

It also specifies a way to minimize the number of exchanges and transferring some long messages – the object_lists – in consideration of the limitations imposed by the lower layers of the communication profile specified in this document. This is achieved by using pre-established Application Associations and defining the list of COSEM objects with their base_names that can be used in actual implementations.

C.2 Client-server model

C.2.1 General

As specified in IEC 62056-5-3:2017, 4.2, DLMS/COSEM is based on the client-server model in which client and server application processes communicate with each other. The clients send service requests to servers and the servers respond to these requests. This takes place within Application Associations, see C.2.4.

In the communication environments targeted by the communication profile specified in this document the client APs are located in the NNAP and server APs are located in LNAPs which may be co-located with the end devices. See also Clause 4, Figure 1.

C.2.2 Clients

A server may be accessed by several clients each using specific contexts and having specific access rights.

IEC 62056-5-3:2017, 4.1.5 specifies three different kinds of contexts:

- the application context that stipulates the referencing style of COSEM object attributes and methods and the use of ciphering;
- the authentication context, that stipulates the method and algorithms to authenticate the client and the server;
- the xDLMS context that stipulates the set of xDLMS services to be used and some other parameters.

The access rights determine the list of COSEM objects visible in a given AA, together with the access rights to their attributes and methods, as well as the required protection of the service requests and responses.

There shall be at least one public client implemented. Its role is revealing the internal structure of the servers. It has a pre-defined Service Access Point; see Table 2.

See also IEC 62056-5-3:2017, 4.1.14.

C.2.3 Servers

As specified in IEC 62056-6-2:2017, 4.7, the server is a physical device that contains one or more logical devices. Each logical device represents a COSEM application process, which is modelled by a particular set of COSEM objects.

In each physical device, there shall be at least one Management Logical Device implemented that may be the only logical device. It has a pre-defined Service Access Point, see Table 2. See also IEC 62056-5-3:2017, 4.1.9.

C.2.4 Application associations

C.2.4.1 Overview

As specified in IEC 62056-5-3:2017, 4.1.5, information exchange between clients and servers takes place within Application Associations (AA).

A client may be able to establish AAs with one or more servers. Likewise, a server may be able to support AA with one or more clients. Such AA may be simultaneously used or not, depending on the capabilities of the client and the server.

As specified in IEC 62056-5-3:2017, 4.1.5, AAs may be:

- explicitly established or pre-established;
- confirmed or unconfirmed;
- use short name (SN) referencing or logical name (LN) referencing to COSEM object attributes and methods with or without ciphering;
- use various authentication mechanisms;
- use various different xDLMS contexts;

The AAs are modelled with the Association objects, see IEC 62056-6-2:2017, 5.3.3. and 5.3.4. Each AA is identified by a pair of client and server SAPs.

C.2.4.2 Explicitly established AAs

Explicitly established AAs are established using the COSEM-OPEN service specified in IEC 62056-5-3:2017, 6.2. This involves an exchange of the ACSE AARQ and AARE APDUs to negotiate the application context, the authentication context and the xDLMS context. In the case of authentication using High Level Security an additional exchange is required to exchange the result of the processing of the challenge by the peer.

C.2.4.3 Pre-established AAs

As specified in IEC 62056-5-3:2017, 4.1.4, AAs may also be pre-established. This means that the contexts of the AA are pre-defined and known by the client and the server that wish to use them.

When using pre-established AAs, the exchanges to establish the AAs can be avoided. However, several features are not available:

- authentication of the peers using passwords or challenges;
- client user identification;
- exchanging public key certificates with the AARQ/ARRE exchange.

See also IEC 62056-5-3:2017, 6.2.

Table C.1 specifies a pre-established AA – that may be used, but not mandatory – between Client with SAP = 0x7D and the Management Logical Device with SAP = 0x01.

Table C.1 – Pre-established association parameters

Parameter	Value
Client SAP	0x7D
Server SAP	0x01
Application context name	Short_Name_Referencing_With_Ciphering joint-iso-ccitt(2) country(16) country-name(756) identified-organisation(5) DLMS-UA(8) application-context(1) context_id(4)}
xDLMS version	0x06
Client Maximum PDU Size	58
Server Maximum PDU Size	82
Conformance block	• general-protection (1) • general-block-transfer (2) • read (3) • write (4) • unconfirmed-write (5) • parameterized-access (18)

The objects visible in this association:

- shall contain the mandatory objects as specified in C.3.4;
- the utility table objects specified in Table C.3;
- the security related objects as specified in C.3.5, with their class_id, version, base_name and access rights;
- any other object required for the application with their class_id, version, base_name and access rights.

C.2.4.4 The mandatory public AA

One AA is mandatory: this is the public AA between the Public client and the Management Logical Device. It shall support an AA to a public client with an application context without ciphering and with lowest level security (no security) authentication. Its role is to support revealing the internal structure of the physical device and to support notification of events in the server. See also IEC 62056-6-2:2017, 4.8.5.

NOTE Notifications by the server are not supported in the communication profile specified in this document.

Since the public AA does not provide security it may be used for accessing non-sensitive information only.

C.2.4.5 Other AAs

In addition to the mandatory public AA, any other explicitly established or pre-established AAs may be specified using the application context, authentication context, xDLMS context and object_list as required.

C.3 The COSEM objects

C.3.1 COSEM object model

The COSEM object model is specified in IEC 62056-6-2:2017.

As specified in IEC 62056-6-2:2017, 4.1, a COSEM object is a collection of attributes and methods. Attributes represent the characteristics of an object. The value of an attribute can affect the behaviour of an object. The first attribute of any object is the `logical_name`. It is one part of the identification of the object. An object may offer a number of methods to either examine or modify the values of the attributes.

Objects that share common characteristics are generalized as an interface class, identified with a `class_id`. An interface class may have one or more versions.

To exchange data, attributes and methods of the COSEM objects have to be accessed.

C.3.2 Referencing methods

As specified in IEC 62056-5-3:2017, 4.2.4.3, there are two referencing methods (styles) available to reference COSEM object attributes and methods:

- short name (SN) referencing; and
- logical name (LN) referencing.

The client always uses LN referencing. The server may use LN or SN referencing (or both).

When LN referencing is used, COSEM object attributes and methods are accessed with the xDLMS service requests using LN referencing: the GET, SET, ACTION and ACCESS services. They are specified IEC 62056-5-3:2017, 6.6 to 6.9.

The LN service requests contain an attribute or method descriptor that is composed of the `class_id`, the `logical_name` (i.e. the OBIS code) and the attribute or method ID. An attribute or method descriptor is expressed on 9 bytes.

When SN referencing is used, each COSEM object attribute and method is mapped to a COSEM named variable, expressed on two bytes.

As specified in IEC 62056-5-3:2017 Clause 8, the short names are of type Integer16 with last three bits set to 0. With this, the range of short names is from 0x0008 to 0x FFF8 and there are 8 191 variable names available.

The `logical_name` attribute of each COSEM object instance is mapped to an implementation specific `base_name` that can be retrieved by reading the `object_list` attribute of the Association SN object(s). For some objects, the `base_name` is standardised. `Base_names` may also be specified in companion specifications.

The offsets for the other attributes and methods are specified in the COSEM interface class specifications.

COSEM object attributes and methods are accessed then with the xDLMS service requests using SN referencing: the Read or Write xDLMS services. They are specified in IEC 62056-5-3:2017, 6.12 to 6.14. The SN service requests include the base name.

As already mentioned above, the client always uses LN referencing. Therefore, if the server uses SN referencing the Client SN_Mapper Application Service Element (ASE) in the client maps the LN service primitives to SN service primitive and vice versa. The mappings are specified in IEC 62056-5-3:2017, 7.3.9 to 7.3.11.

Service requests using short name referencing are shorter than the ones using logical name referencing. However, this difference is there only in the service requests, as the attribute and method descriptors are present only in the request.

On the other hand, on the client side, a translation between APDUs using LN referencing and SN referencing has to be performed for each request and response.

Example: A GET-request APDU containing the COSEM-Attribute-Descriptor has to be translated to a Read.request APDU containing the variable name to which the COSEM-Attribute-Descriptor has been mapped.

C.3.3 The object_list

In order to communicate with the server, the client needs to know the method to reference the COSEM object attributes and methods in the service requests.

It also has to know:

- the list of COSEM objects accessible in each AA;
- in the case of SN referencing, the base_name of each object; and
- the access rights to each attribute and method.

This information can be read from the Association LN / Association SN objects; see IEC 62056-6-2:2017, 5.3.3 and 5.3.4.

The object_list may also be specified in project specific companion specifications.

C.3.4 Mandatory COSEM objects

As specified in IEC 62056-6-2:2017, 4.8.4, the following objects shall be present in each COSEM logical device. They shall be accessible for GET/Read in all AAs with this logical device:

- COSEM logical device name object;
- current Association object, "Association SN" or "Association LN" in line with the referencing method used.

If there are several logical devices, a SAP assignment object has to be present in the management Logical Device. In this case, the COSEM logical device name object does not have to be present.

The reserved base_names of the mandatory objects are specified in IEC 62056-6-2:2017, 4.3.

C.3.5 Application specific objects

The other COSEM objects may be implemented according to functionality required.

To support cryptographic protection of xDLMS APDUs the following objects are necessary:

- Security setup objects, see IEC 62056-6-2:2017, 5.3.7;
- Invocation counter objects, see IEC 62056-6-2:2017, 6.2.33.

To support COSEM data protection, Data protection objects, see IEC 62056-6-2:2017, 5.3.9.

C.3.6 Utility table objects

IEC 62056-6-2:2017, 5.2.7 specifies Utility table objects that allow encapsulating ANSI C12.19 Utility Industry End Device Data Tables AKA "Utility tables". Each Utility table is represented by an instance of this IC, identified by its logical name. The OBIS codes of Utility tables are specified in IEC 62056-6-2:2017, 6.2.36.

Using these Utility table objects provides a migration path from applications using the ANSI C12.19 tables to DLMS/COSEM: the Utility table objects may co-exist with other COSEM objects in the same or in different AAs and the data held in the tables can be accessed by DLMS/COSEM services.

ANSI C12.19 specifies:

- 2 048 Standard tables (table identifier range 0 to 2 047);
- 2 048 Manufacturer tables (table identifier range 2 048 to 4 095);
- 2 048 Standard pending tables (table identifier range 4 096 to 6 143);
- 2 048 Manufacturer pending tables (table identifier range 6 144 to 8 191).

There are also user-defined tables.

To use the tables with SN referencing, the attributes of the Utility table objects have to be mapped to short names. As each Utility table object has 4 attributes, mapping all attributes of Standard and Manufacturer tables to short names would require 32 640 named variables, but only 8 191 are available. This limits the number of tables/Utility table objects that can be accessed using SN referencing.

The `base_names` of the Utility tables implemented can be retrieved by reading the `object_list` attribute of the Association SN object that models the AA with the logical device implementing the tables.

To avoid reading the `object_list`, this document specifies `base_names` for selected Utility tables.

Table C.2 specifies the `base_name` ranges available for the four utility table categories.

Table C.2 – `base_name` range for tables categories

Table category	Start base name	End base name	Table Id	COSEM Objects	
				From	To
Standard Tables	0x9000	0x9760	0000 – 79	0-0:65.0.0.255	0-0:65.0.79.255
Manufacturer Tables	0x9800	0xAFF8	0000 – 2047	0-0:65.16.0.255	0-0:65.31.127.255
Standard pending Tables	0xB000	0xB7E0	0000 – 2047	0-0:65.32.0.255	0-0:65.47.127.255
Manufacturer Pending tables	0xB800	0xCFF8	0000 – 2047	0-0:65.48.0.255	0-0:65.63.127.255

Table C.3 defines the `base_name` for the first Standard tables, named BT00 up to BT79.

In the scope of this document, reading the `object_list` from the server can be avoided if it is known in advance, meaning:

- all these standard tables and only these tables are used;
- the `base_name` of all other tables is specified in the companion specification;

NOTE It is assumed that each attribute of the Utility table objects is implemented and the access rights are specified in the companion specification.

- the `base_name`, `interface_class` version and access rights to each attribute and method of all other COSEM objects are specified in the companion specification.

Table C.3 – base_names for standard tables BT00 to BT79

Table ID	OBIS code	base_name	Name
BT00	0-0:65.0.0.255	0x9000	General Configuration
BT01	0-0:65.0.1.255	0x9020	General Manufacturer Identification
BT02	0-0:65.0.2.255	0x9040	Device Nameplate
BT03	0-0:65.0.3.255	0x9060	End Device Mode Status
BT04	0-0:65.0.4.255	0x9080	Pending Status
BT05	0-0:65.0.5.255	0x90A0	Device Identification
BT06	0-0:65.0.6.255	0x90C0	Utility Information
BT07	0-0:65.0.7.255	0x90E0	Procedure Initiate
BT08	0-0:65.0.8.255	0x9100	Procedure response
BT10	0-0:65.0.10.255	0x9120	Dimension Source Limiting
BT11	0-0:65.0.11.255	0x9140	Actual sources limiting
BT12	0-0:65.0.12.255	0x9160	Unit of Measure Entry
BT13	0-0:65.0.13.255	0x9180	Demand Control
BT15	0-0:65.0.15.255	0x91A0	Constants
BT16	0-0:65.0.16.255	0x91E0	Source definition
BT17	0-0:65.0.17.255	0x9200	Alternate source definition
BT20	0-0:65.0.20.255	0x9220	Dimension Register
BT21	0-0:65.0.21.255	0x9240	Actual Register
BT22	0-0:65.0.22.255	0x9260	Data Selection
BT23	0-0:65.0.23.255	0x9280	Current Register Data
BT24	0-0:65.0.24.255	0x92A0	Previous Season Data
BT25	0-0:65.0.25.255	0x92C0	Previous Demand Reset
BT26	0-0:65.0.26.255	0x92E0	Self-Read Data
BT27	0-0:65.0.27.255	0x9300	Present Register Selection
BT28	0-0:65.0.28.255	0x9320	Present Register Data
BT30	0-0:65.0.30.255	0x9340	Dimension Display
BT31	0-0:65.0.31.255	0x9360	Actual Display
BT32	0-0:65.0.32.255	0x9380	Display Source
BT33	0-0:65.0.33.255	0x93A0	Primary Display List
BT40	0-0:65.0.40.255	0x93C0	Dimension Security Limiting
BT41	0-0:65.0.41.255	0x93E0	Actual Security Limiting
BT42	0-0:65.0.42.255	0x9400	Security
BT43	0-0:65.0.43.255	0x9420	Default Access Control
BT44	0-0:65.0.44.255	0x9440	Access Control
BT45	0-0:65.0.45.255	0x9460	Key
BT50	0-0:65.0.50.255	0x9480	Dimension Time and TOU
BT52	0-0:65.0.52.255	0x94A0	Clock
BT53	0-0:65.0.53.255	0x94C0	Time Offset
BT54	0-0:65.0.54.255	0x94E0	Calendar
BT55	0-0:65.0.55.255	0x9500	Clock State
BT56	0-0:65.0.56.255	0x9520	Time Remaining Table
BT60	0-0:65.0.60.255	0x9540	Dimension Load Profile
BT61	0-0:65.0.61.255	0x9560	Actual Load Profile

Table ID	OBIS code	base_name	Name
BT62	0-0:65.0.62.255	0x9580	Load Profile Control
BT63	0-0:65.0.63.255	0x95A0	Load Profile Status
BT64	0-0:65.0.64.255	0x95C0	Load Profile Data 1
BT65	0-0:65.0.65.255	0x95E0	Load Profile Data 2
BT66	0-0:65.0.66.255	0x9600	Load Profile Data 3
BT67	0-0:65.0.67.255	0x9620	Load Profile Data 4
BT70	0-0:65.0.70.255	0x9640	Dimension Log
BT71	0-0:65.0.71.255	0x9660	Actual Log
BT72	0-0:65.0.72.255	0x9680	Event Identification
BT73	0-0:65.0.73.255	0x96A0	History Log Control
BT74	0-0:65.0.74.255	0x96C0	History Log Data
BT75	0-0:65.0.75.255	0x96E0	Event Log Control
BT76	0-0:65.0.76.255	0x9700	Event Log Data
BT77	0-0:65.0.77.255	0x9720	Event Log and Signatures Enable
BT78	0-0:65.0.78.255	0x9740	End Device Program State Table
BT79	0-0:65.0.79.255	0x9760	Event Counters Table

Annex D (informative)

OSGP-AES-128-PSK security suite

D.1 General

The OSGP-AES-128-PSK security suite provides a protected two-way communication channel between a NNAP (DC) and an LNAP (meter). The secure channel provides data confidentiality, data and origin integrity, and replay protection. It can be used for both broadcast communication and unicast communication.

OSGP-AES-128-PSK is specifically designed for constrained-networks of legacy low-end embedded devices.

The security suite consists of three logical layers (1 to 3) as shown in Table D.1.

Table D.1 – Security logical layers

Logical layer	Name	Contents
4	ADP	Upper layer protocol
3	Secure Channel Protocol	Secure channel initialization Secure channel unicast communication Secure channel broadcast communication
2	Cryptographic Functions	OSGP_KDF OSGP_MAC OSGP_MAC_VERIFY OSGP_AE OSGP_AD
1	Cryptographic Primitives	AES-128 CCM CMAC

Each logical layer uses the service of the logical layer beneath it (if any) and provides a service for the logical layer above it (if any). For example, the Secure Channel Protocol logical layer uses the OSGP_AE function provided by the Cryptographic Functions logical layer for protecting messages, which in turn is used to provide secure channel communication to the Adaptation logical layer above.

OSGP-AES-128-PSK requires that an initial pre-shared key has been securely established. How this is done, is outside the scope of this specification.

The specification of OSGP-AES-128-PSK is structured, based on the reverse order of the logical layers. Specifically, the remainder of this Annex is structured into the following top-level clauses:

- Background: sets the stage for the security suite by describing the target system, the threat model, and the design goals for the security suite;
- Terms and notation: describes the terms and notation used throughout this specification;
- Cryptographic primitives: specifies the low-level cryptographic primitives that act as building blocks for the security suite;

- Cryptographic functions: specifies the high-level cryptographic functions referenced in the protocol specification;
- Keys: specifies the keys and the key hierarchy in the cryptographic system;
- Secure channel initialization: specifies how a secure channel is established;
- Secure channel communication: specifies how the secure channel is used to protect network communication;
- Key management: specifies how keys are generated, distributed and renewed, and the recommended key validity periods;
- Error messages: specifies the common security-related error messages used to indicate failures in the protocol;
- Security considerations: provides additional recommended practices with respect to this security suite as well as reasoning behind the security suite's design;
- References: lists the literature cited throughout this document.

D.2 Background

D.2.1 Overview

This clause provides background information about the target system, the threat model considered, the design goals, and the inspiration for this security suite.

D.2.2 System Assumptions

The system assumption is a list of important assumptions about the target system.

- The target system is a network of legacy embedded devices that are 10 to 15 years old. Thus, LNAPs and NNAPs are expected to be significantly resource-constrained, both in terms of memory and computing power.
- The communication network is bandwidth-constrained, throughput-constrained, noisy, and substantially prone to data corruption during transfers, thus often requiring retries to complete a transaction.
- The communication medium is shared between a subnet of nodes (up to 1 024) and can thus only be used by one node at a time. Attempts at concurrent communication results in packet corruption.
- The underlying transport protocol cannot be modified.
- To address the problem of the shared medium, the NNAP is the only initiator of communication. That way, under normal network activity, a NNAP is able to control the use of the medium.

D.2.3 Threat Model

This security suite is concerned with a network adversary that has complete control over the communication network and knows everything about the cryptographic system except for the secret keys.

The adversary is assumed to have access to high-performance computing resources.

Although mounting man-in-the-middle attacks on a shared medium network may be difficult in practice, the adversary is assumed to be able to record, tamper, drop, and/or inject messages arbitrarily at any point in time in the protocol.

It is important to pay attention to the fact that the adversary is under the same constraints imposed by the low-performing network, just like all the other nodes on the network.

D.2.4 Design goals

The goals of this security suite are as follows:

- **Security:** the security suite should be conservative in its cryptographic design and follows modern best practices and recommendations from cryptographers and security experts. The security should be defined, as a minimum, by the secrecy of the cryptographic keys used.
- **Secure communication:** the security suite should provide:
 - a) **Message confidentiality:** it should not be feasible to read any secure communication unless you have access to the (encryption) key being used.
 - b) **Message origin integrity (authenticity):** it should be possible to verify the origin of a given message based on a shared secret.
 - c) **Message data integrity:** it should be possible to verify that a given message has not changed since it was generated based on a shared secret.
 - d) **Message replay prevention:** it should be possible to detect and reject replayed (old) messages.
 - e) **Message reflection prevention:** it should be possible to detect and reject messages that are being redirected from its original destination to a new destination.
- **LNAP compartmentalization:** the security suite should provide means to limit the impact of LNAP (key) compromises as much as possible.
- **Developer friendly:** it should be straightforward for developers to program a secure, efficient, and relatively small implementation of the security suite.
- **Suitable for legacy, resource-constrained devices on slow communication networks:**
 - f) **Minimal implementation footprint:** the size of the security suite implementation should be small compared to other security solutions with similar design goals while still achieving acceptable speeds. This is to cater for the memory-constrained devices in the target system.
 - g) **Minimal computational overhead:** the security suite should run at acceptable speeds on 10 to 15-year-old embedded devices. That is, the computational overhead of using this security suite should not degrade the performance to unacceptable levels.
 - h) **Minimal network overhead:** the security suite should reduce the cryptographic overhead per network packet and the number of packets needed as much as possible to cater for the possibility of a slow and unreliable target system network.

D.2.5 Inspiration

This security suite is to a great extent based on the Pre-Shared Key Extensible Authentication Protocol (EAP) IETF RFC 5433 as specified in IEEE Std 802.11ac-2013. Both of these established protocols share similar design goals with OSGP-AES-128-PSK. Note that CCMP-128 is largely considered secure in the industry (e.g. CCMP-128's use is included in NIST's Suite B Cryptography as of 2015).

D.3 Terms, definitions, abbreviated terms and notation

D.3.1 Terms and definitions

D.3.1.1

associated data

data that is authenticated but not encrypted

D.3.1.2

byte

string of 8 bits