DIN EN IEC 62056-8-8 (VDE 0418-6-8-8)

DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

VDE

ICS 33.200; 35.240.99; 91.140.50

Datenkommunikation der elektrischen Energiemessung – DLMS/COSEM – Teil 8-8: Kommunikationsprofil für Netzwerke der Reihe ISO/IEC 14908 (IEC 62056-8-8:2020); Englische Fassung EN IEC 62056-8-8:2020

Electricity metering data exchange –
The DLMS/COSEM suite –
Part 8-8: Communication profile for ISO/IEC 14908 series networks
(IEC 62056-8-8:2020);
English version EN IEC 62056-8-8:2020

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
(IEC 62056-8-8:2020);
Version anglaise EN IEC 62056-8-8:2020

Gesamtumfang 107 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2020-06-02 angenommene Europäische Norm als DIN-Norm ist 2021-07-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62056-8-8 (VDE 0418-6-8-8):2017-12.

Für dieses Dokument ist das nationale Arbeitsgremium K 461 „Messeinrichtungen und -systeme für Elektrizität" der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Bei diesem Dokument handelt es sich wie bei der enthaltenen IEC-Publikation um die Edition 1.

Die enthaltene IEC-Publikation wurde vom TC 13 „Electrical energy measurement and control" erarbeitet und unterliegt dem Copyright der IEC.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „http://webstore.iec.ch" zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument
- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN IEC 62056-8-8 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt und Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. Weder das Deutsche Komitee, noch IEC, noch CENELEC sind dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

Nationaler Anhang NA
(informativ)

Auszugsweise Übersetzung

Reihenfolge und Inhalt der folgenden Abschnitte sind identisch mit denen in den jeweiligen Abschnitten der Englischen Fassung.

1 Anwendungsbereich

Dieser Teil von IEC 62056 beschreibt, wie die DLMS/COSEM-Anwendungsschicht und das COSEM-Objektmodell nach IEC 62056-5-3:2017, IEC 62056-6-1:2017 und IEC 62056-6-2:2017 über den in der Normenreihe IEC 14908 festgelegten unteren Schichten verwendet werden können und ein ISO/IEC 14908 entsprechendes DLMS/COSEM-Kommunikationsprofil bilden.

Dieses Dokument ist Teil der Normenreihe IEC 62056. Sein Aufbau entspricht IEC 62056-1-0 und IEC TS 62056-1-1.

Anhang A (informativ) gibt Beispiele für repräsentative Anwendungsfälle des Datenaustauschs.

ANMERKUNG Dieser Anhang A wurde aufgenommen und zitiert, um Übereinstimmung mit anderen Teilen der Reihe IEC 62056 zu erzielen, er ist aber leer.

Anhang B (informativ) legt die COSEM-Schnittstellenklassen und die zugehörigen OBIS-Codes für die Einstellung und die Verwaltung des DLMS/COSEM-Kommunikationsprofils für Netzwerke der Reihe IEC 14908 fest. Diese Schnittstellenklassen und OBIS-Codes werden später in IEC 62056-6-2 und IEC 62056-6-1 überführt.

Anhang C (informativ) enthält einen Implementierungsleitfaden und legt einen Migrationspfad von den auf den Tabellen der Versorgungseinrichtung (Utility-Tabellen) basierenden Anwendungen zu DLMS/COSEM-basierten Anwendungen fest.

Anhang D (informativ) legt die OSGP-AES-128-PSK-Sicherheitssuite zur optionalen Verwendung auf der Ebene der Adaptionsschicht fest.

Anhang E (normativ) legt den Wiederholungsmechanismus über das Kommunikationsnetz über die Stromversorgungsleitungen nach ISO 14908-3 fest.

Anhang F (informativ) legt die Registrierung und Überwachung von LNAPs nach ISO/IEC 14908-3 fest.

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe und Abkürzungen.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

– IEC Electropedia: verfügbar unter http://www.electropedia.org/

– ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

ANMERKUNG Alle Nachrichten in diesem Dokument verwenden das Big-Endian-Format.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

3.1 Begriffe

3.1.1
Domäne
(en: domain)
logisches Netzwerk als Einheit für eine Adressierung

Anmerkung 1 zum Begriff: Subnetz- (siehe unten) und Knotenadressen werden von dem für die Domäne verantwortlichen Administrator zugewiesen und haben nur im Zusammenhang mit dieser Domäne eine Bedeutung.

Anmerkung 2 zum Begriff: Alle Knoten gehören zur selben Domäne, um sich gegenseitig adressieren zu können.

3.1.2
Knoten
(en: node)
Abstraktion für einen physikalischen Knoten, der den höchsten Grad der Adresslösbarkeit in einem Netzwerk besitzt

Anmerkung 1 zum Begriff: Ein Knoten ist innerhalb eines Subnetzes durch seinen (logischen) Knotenbezeichner gekennzeichnet (adressiert), der als Node_ID bezeichnet wird. Ein physikalischer Knoten kann gegebenenfalls zu mehr als einem Subnetz gehören; wenn dies der Fall ist, wird ihm eine (logische) Knoten-Nummer für jedes Subnetz, zu dem er gehört, zugewiesen. Ein physikalischer Knoten kann gegebenenfalls zu höchstens zwei Subnetzen gehören; diese Subnetze liegen in unterschiedlichen Domänen. Ein Knoten kann gegebenenfalls auch innerhalb eines Netzwerks mithilfe seiner unveränderlichen Unique_Node_ID (absolut) gekennzeichnet werden.

3.1.3
Subnetz
(en: subnet)
Reihe von Knoten, die über dasselbe Sicherungsschicht-Protokoll zugänglich sind

Anmerkung 1 zum Begriff: In einer logischen Adresse wird ein Subnetz durch eine Subnet_ID gekennzeichnet.

3.1.4
Transaktion
(en: transaction)
Folge von Nachrichten, die miteinander in Beziehung stehen

Anmerkung 1 zum Begriff: Beispielsweise eine Anforderung und die Antworten auf die Anforderung sind alle Teil einer einzelnen Transaktion. Eine Transaktion ist erfolgreich, wenn alle erwarteten Nachrichten von jedem an der Transaktion beteiligten Knoten mindestens einmal empfangen werden. Eine Transaktion scheitert, wenn eine der erwarteten Nachrichten bei der Transaktion nicht empfangen wird.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

3.2 Abkürzungen

Abkürzung	Bedeutung	
AA	Anwendungsassoziation	(en: application association)
AARE	Anwendungsassoziationsantwort	(en: application association response)
AARQ	Anwendungsassoziationsanforderung	(en: application association request)
ACSE	Dienstelement der Assoziationssteuerung	(en: association control service element)
ADD	automatisierte Geräteerkennung	(en: automated device discovery)
AdpPDU	PDU der Adaptionsschicht	(en: adaptation layer PDU)
AL	Anwendungsschicht	(en: application layer)
AP	Anwendungsprozess	(en: application process)
APDU	Protokolldateneinheit der Anwendungsschicht	(en: application protocol data unit)
ASE	Anwendungsdienstelement	(en: application service element)
ATM	automatisierte Topologieverwaltung	(en: automated topology management)
BPSK	binäre Phasenumtastung	(en: binary phase shift keyed)
COSEM	Firmenspezifikation für die Gebührenerfassung des Energieverbrauchs	(en: Companion Specification for Energy Metering)
CRC	zyklische Redundanzprüfung	(en: cyclic redundancy check)
CSMA	Medienzugriff mit Trägerprüfung	(en: carrier sense medium access)
DC	Datenkonzentrator	(en: data concentrator)
DLPDU	Protokolldateneinheit der Sicherungsschicht	(en: data link protocol data unit)
DLMS	standardisierte Sprache für die Zählerkommunikation	(en: Device Language Message Specification)
FCM	Nachricht der schnellen Inbetriebnahme	(en: fast commission message)
KMS	Schlüsselverwaltungsystem	(en: key management system)
HES	Datenerfassungssystem	(en: head end system)
LNAP	Zugangspunkte eines lokalen Netzwerks	(en: local network access points)
MAC	Medienzugriffssteuerung (Teilschicht)	(en: medium access control (sublayer))
MAC	Nachrichtenauthentifizierungscode (Kryptografie)	(en: message authentication code (cryptography))
MEP	Mehrzweck-Erweiterungsport	(en: multipurpose expansion port)
NMS	Netzwerkverwaltungssystem	(en: network management system)
NN	Nachbarschaftsnetzwerk	(en: neighbourhood network)
NNAP	Zugangspunkte eines Nachbarschaftsnetzwerks	(en: neighbourhood network access point)
OBIS	Objektidentifikationssystem	(en: Object Identification System)
OSGP	firmenneutrales Smart-Grid-Protokoll	(en: open smart grid protocol [a])
OSI	Kommunikation offener Systeme	(en: open system Information)
PID	Programmkennung	(en: program identifier)
PLC	Trägerfrequenzübertragung über Stromversorgungsleitungen	(en: power line carrier)
PSK	vorinstallierter Schlüssel	(en: pre-shared key)
SAP	Dienstzugangspunkt	(en: service access point)

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

Abkürzung	Bedeutung	
SDU	Dienstdateneinheit	(en: service data unit)
SICB	Dienstschnittstellen-Steuerblock	(en: service interface control block)
UNID	eindeutiger Knotenbezeichner	(en: unique node identifier)
xDLMS	erweiterte DLMS	(en: extended DLMS)

a) OSGP ist ein Geschäftsmodell, das ein Verfahren definiert, wie Smart Metering implementiert werden sollte, und umfasst eine Vielzahl von Elementen und Parametern, einschließlich Sicherheitsauslegung und -implementierung, Datenformate, Datenmodell, Gerätefunktionalitäten.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62056-8-8

June 2020

ICS 17.220; 35.110; 91.140.50

English Version

Electricity metering data exchange – The DLMS/COSEM suite – Part 8-8: Communication profile for ISO/IEC 14908 series networks (IEC 62056-8-8:2020)

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 (IEC 62056-8-8:2020)

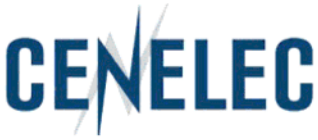
Datenkommunikation der elektrischen Energiemessung – DLMS/COSEM – Teil 8-8: Kommunikationsprofil für Netzwerke der Reihe ISO/IEC 14908 (IEC 62056-8-8:2020)

This European Standard was approved by CENELEC on 2020-06-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62056-8-8:2020 E

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

European foreword

The text of document 13/1783/CDV, future edition 1 of IEC 62056-8-8, prepared by IEC/TC 13 "Electrical energy measurement and control" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62056-8-8:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2021-03-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-06-02

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62056-8-8:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 62056-1-0 NOTE Harmonized as EN 62056-1-0

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 62056-5-3	2017	Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer	EN 62056-5-3	2017
IEC 62056-6-1	2017	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: Object Identification System (OBIS)	EN 62056-6-1	2017
IEC 62056-6-2	2017	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-2: COSEM interface classes	EN IEC 62056-6-2	2018
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	-	-
-	-	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	EN 50065-1	-

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

CONTENTS

European foreword 2
Annex ZA (normative) Normative references to international publications with their corresponding European publications 3
INTRODUCTION 10
1 Scope 11
2 Normative references 11
3 Terms, definitions and abbreviated terms 12
3.1 Terms and definitions 12
3.2 Abbreviated terms 5
4 Targeted communication environments 14
5 Use of the communication layers for this profile 14
5.1 Information related to the use of the standard specifying the lower layers 14
5.2 The structure of the communication profile 15
5.3 Lower layers and their use 15
5.3.1 Overview 15
5.3.2 Physical layer 16
5.3.3 Data link layer 16
5.3.4 Network layer 16
5.3.5 Transport layer 16
5.4 Service mapping and Adaptation layer 17
5.4.1 Overview 17
5.4.2 Adaptation layer 17
5.5 Registration and connection management 28
6 Identification and addressing schemes 28
7 Specific considerations for the application layer services 29
7.1 Overview 29
7.2 Application Association establishment and release: ACSE services 29
7.2.1 Application association establishment 29
7.2.2 Application association release 30
7.2.3 COSEM-OPEN and COSEM-RELEASE service parameters 30
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 31
7.5 Transferring long application messages 31
7.6 Media access, bandwidth and timing considerations 31

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

7.7 Other considerations 31
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 51
D.4 Cryptographic Primitives 51

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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 ... 78
D.11.1 General ... 78
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 ... 79
D.13.1 Reasoning ... 79
D.13.2 Recommendation and Guidance for Implementers ... 81

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

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 84
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 87
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 95
F.4.1 General 95
F.4.2 ATM roles 95
F.4.3 Automatic discovery 96
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 14
Figure 2 – Structure of the communication profile 15
Figure 3 – Adaptation layer structure 18
Figure 4 – Unprotected Adaptation layer PDU structure 19

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

Figure 5 – Protected Adaptation layer PDU structure 20
Figure 6 – Adaptation layer services 21
Figure 7 – Client and server ADP_DATA services 24
Figure D.1 – Key hierarchy diagram 55
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 86
Figure E.5 – Proxy Repeater proxy message 87
Figure E.6 – Proxy Agent proxy message format 87
Figure E.7 – Proxy Target message format 87
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 19
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

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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

NOTE Harmonized as EN 62056-1-0.

IEC TS 62056-1-1 for its structure.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

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
NOTE Harmonized as EN 62056-1-0.

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*

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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.

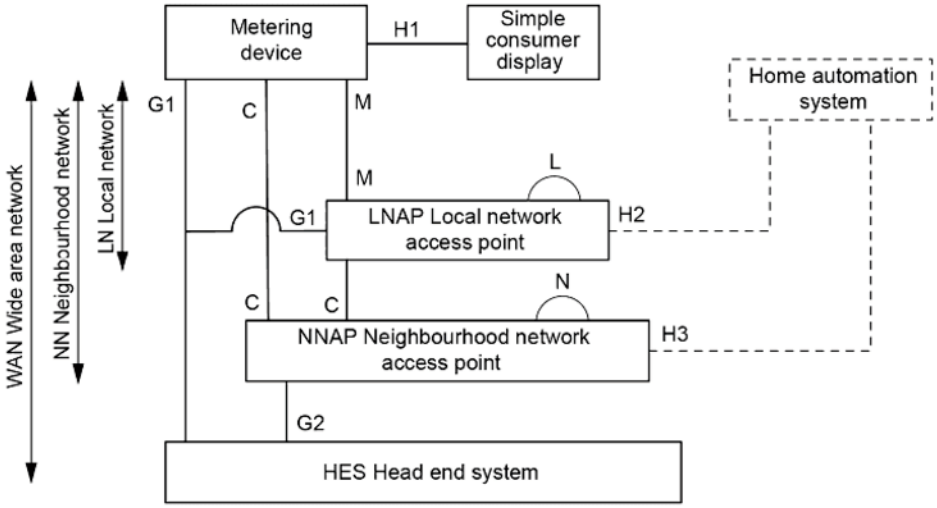


Figure 1 – Functional reference architecture

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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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.

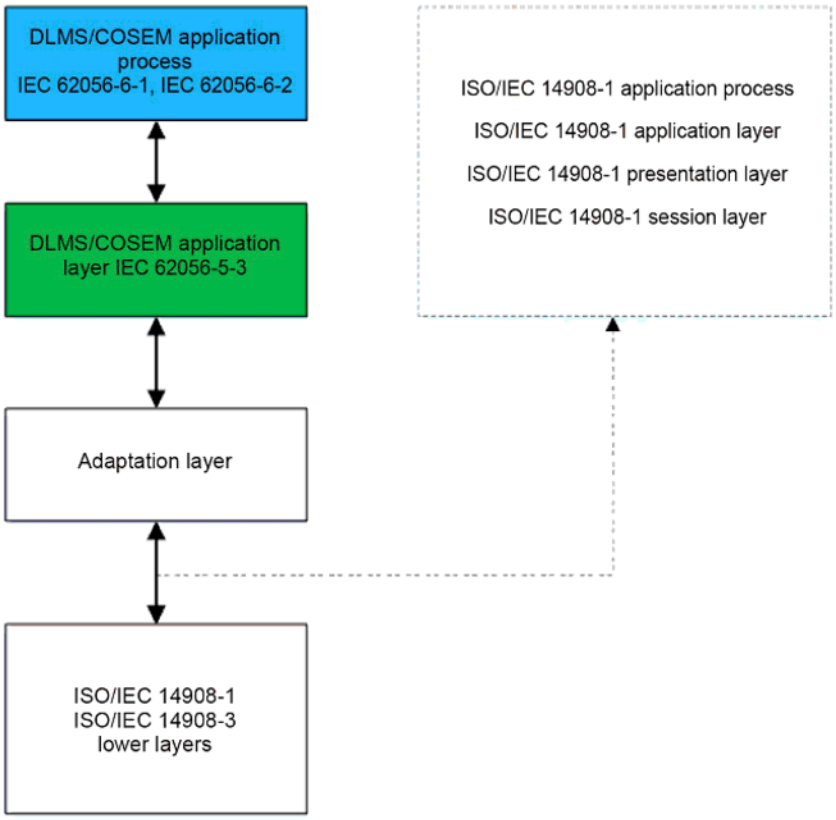


Figure 2 – Structure of the communication profile

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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

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 0;
- to redirect the messages to the DLMS/COSEM Application layer depending on the value of the control field during the message reception, see 0;
- to provide the required addressing parameters for the client application process and the logical device, see 0 items 3 and 4;
- to provide the parameters allowing the correct binding of the higher layer protocol with the Transport layer, see 0;
- 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 0.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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.

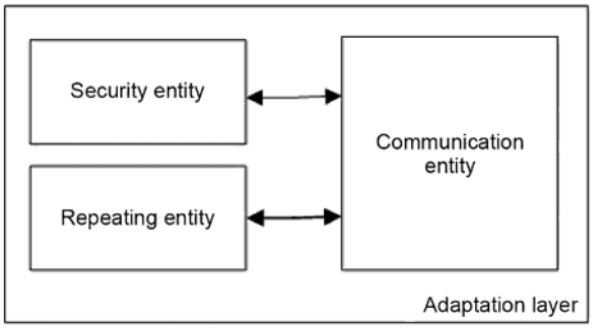


Figure 3 – Adaptation layer structure

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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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:

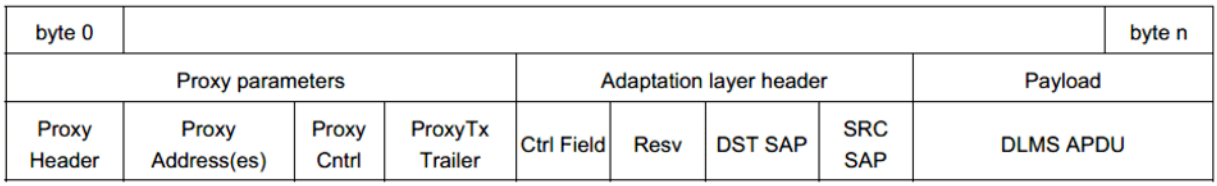


Figure 4 – Unprotected Adaptation layer PDU structure

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:

a) The Ctrl field has a fixed value set to 0x20;

b) 'Resv' field is of one byte and is reserved for future. It shall be set to 0;

c) '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;

d) '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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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.

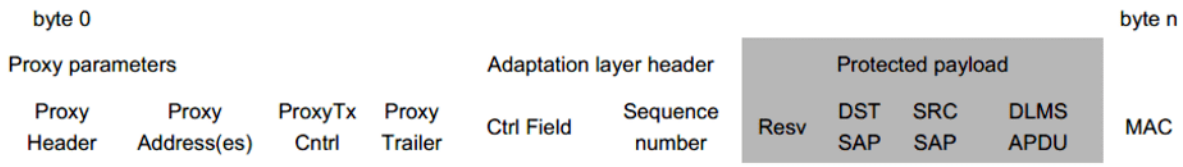


Figure 5 – Protected Adaptation layer PDU structure

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.6, and Table D.8) 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 0 and 0, 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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

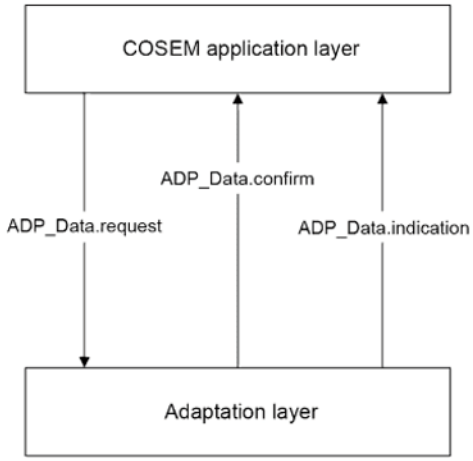


Figure 6 – Adaptation layer services

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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

Table 2 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.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

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 0.

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 0.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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 0.

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.

1.1.1.1 Protocol specification

1.1.1.1.1 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.

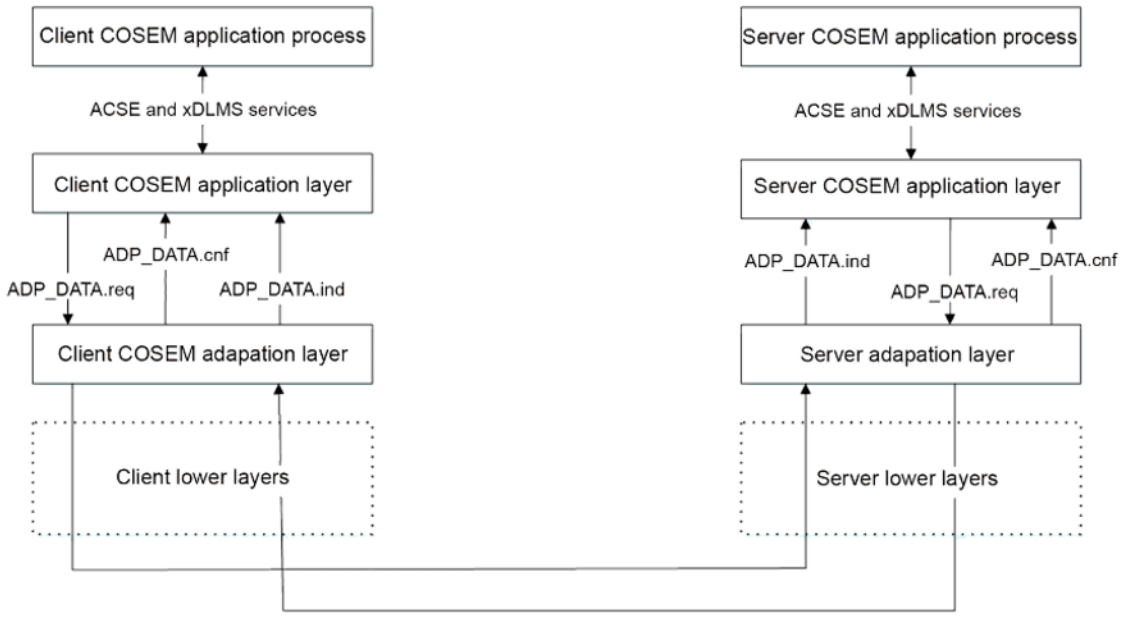


Figure 7 – Client and server ADP_DATA services

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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 0. 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 0, 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 LNAP, 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 LNAP. 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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07

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 0 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;

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62056-8-8:2021-07

- 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.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62056-8-8:2021-07