

DIN EN 62056-5-3/A1

ICS 35.100.70; 91.140.50

Einsprüche bis 2015-04-20
Vorgesehen als Änderung von
DIN EN 62056-5-3:2014-09**Entwurf****Datenkommunikation der elektrischen Energiemessung –
DLMS/COSEM –****Teil 5-3: DLMS/COSEM-Anwendungsschicht
(IEC 13/1571/CDV:2014);****Englische Fassung EN 62056-5-3:2014/FprA1:2014**

Electricity metering data exchange –
The DLMS/COSEM suite –
Part 5-3: DLMS/COSEM application layer
(IEC 13/1571/CDV:2014);
English version EN 62056-5-3:2014/FprA1:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-02-20 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 49 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die Englische Fassung des europäischen Dokuments EN 62056-5-3:2014/FprA1:2014 „Datenkommunikation der elektrischen Energiemessung – DLMS/COSEM – Teil 5-3: DLMS/COSEM-Anwendungsschicht“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 13/1571/CDV:2014 „Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer“ unverändert in den Entwurf EN 62056-5-3:2014/FprA1:2014 übernommen worden.

Das internationale Dokument wurde vom TC 13 „Equipment for electrical energy measurement and load control“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium K 461 „Elektrizitätszähler“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnichtsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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 des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die englische Fassung der EN 62056-5-3:2014/FprA1:2014 veröffentlicht. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

CONTENTS

0			
1	INTRODUCTION.....		7
2	1 Scope.....		8
3	2 Normative references		8
4	3 Terms, definitions and abbreviations		8
5	3.1 Terms and definitions.....		8
6	3.2 Abbreviations		8
7	4 Overview		8
8	4.1 DLMS/COSEM application layer structure		8
9	4.2 DLMS/COSEM application layer services		8
10	4.2.1 ASO services.....		8
11	4.2.2 Services provided for application association establishment		
12	and release		8
13	4.2.3 Services provided for data transfer		9
14	4.2.4 Layer management services		11
15	4.2.5 Summary of DLMS/COSEM application layer services		11
16	4.3 DLMS/COSEM application layer protocols.....		11
17	5 Information security in DLMS/COSEM		12
18	5.1 Definitions.....		12
19	5.2 General.....		12
20	5.3 Data access security.....		12
21	5.3.1 Overview		12
22	5.3.2 No security (lowest level security) authentication		12
23	5.3.3 Low Level Security (LLS) authentication		12
24	5.3.4 High Level Security (HLS) authentication		12
25	5.4 Data transport security.....		14
26	5.4.1 Applying, removing or checking the protection: ciphering and		
27	deciphering.....		14
28	5.4.2 Security context.....		14
29	5.4.3 Security policy		14
30	5.4.4 Security suite.....		14
31	5.4.5 Security material.....		14
32	5.4.6 Ciphered xDLMS APDUs		14
33	5.4.7 Cryptographic keys.....		16
34	5.4.8 The Galois/Counter Mode of Operation (GCM).....		16
35	6 DLMS/COSEM application layer service specification		20
36	6.1 Service primitives and parameters		20
37	6.2 The COSEM-OPEN service.....		20
38	6.3 The COSEM-RELEASE service.....		20
39	6.4 The COSEM-ABORT service.....		20
40	6.5 Protection and general block transfer parameters		20
41	6.6 The GET service		24
42	6.7 The SET service		24
43	6.8 The ACTION service		24
44	6.9 The EventNotification service.....		24
45	6.10 The TriggerEventNotificationSending service		24
46	6.11 Variable access specification		24

47	6.12	The Read service	24
48	6.13	The Write service	24
49	6.14	The UnconfirmedWrite service	24
50	6.15	The InformationReport service	24
51	6.16	The DataNotification service	24
52	6.17	Client side layer management services: the SetMapperTable.request	25
53	6.18	Summary of services and LN/SN data transfer service mapping	26
54	7	DLMS/COSEM application layer protocol specification	27
55	7.1	The control function	27
56	7.2	The ACSE services and APDUs	27
57	7.2.1	ACSE functional units, services and service parameters	27
58	7.2.2	Registered COSEM names	27
59	7.2.3	APDU encoding rules	27
60	7.2.4	Protocol for application association establishment	27
61	7.2.5	Protocol for application association release	27
62	7.3	Protocol for the data transfer services	27
63	7.3.1	Negotiation of services and options – the conformance block	27
64	7.3.2	Confirmed and unconfirmed service invocations	28
65	7.3.3	Protocol for the GET service	28
66	7.3.4	Protocol for the SET service	28
67	7.3.5	Protocol for ACTION service	28
68	7.3.6	Protocol for the EventNotification service	28
69	7.3.7	Protocol for the Read service	28
70	7.3.8	Protocol for the Write service	28
71	7.3.9	Protocol for the UnconfirmedWrite service	29
72	7.3.10	Protocol for the InformationReport service	29
73	7.3.11	Protocol of the DataNotification service	29
74	7.3.12	Protocol of general block transfer mechanism	29
75	8	Abstract syntax of ACSE and COSEM APDUs	39
76	Annex A (normative)	Using the DLMS/COSEM application layer in various	
77		communications profiles	42
78	Annex B (normative)	SMS short wrapper	43
79	Annex C (informative)	AARQ and AARE encoding examples	44
80	Annex D (informative)	Encoding examples: AARQ and AARE APDUs using a ciphered	
81		application context	45
82	Annex E (informative)	Data transfer service examples	46
83	Annex F (informative)	Overview of cryptography	47
84	Annex G (informative)	Significant technical changes with respect to IEC 62056-53	48
85	BIBLIOGRAPHY		49
86			
87	Figure 1 (Replacing Figure 2) – Summary of DLMS/COSEM AL services		11
88	Figure 2 (Replacing Figure 3) – Authentication mechanisms during AA establishment		13
89	Figure 3 – Structure of service specific global ciphering and dedicated ciphering		
90	APDUs		15
91	Figure 4 – Structure of general global ciphering and dedicated ciphering APDUs		15
92	Figure 5 (Replacing Figure 6) – Cryptographic protection of xDLMS APDUs using GCM		17
93	Figure 6 – Additional service parameters to control cryptographic protection and		
94	general block transfer		21

95	Figure 7 – Partial service invocations and GBT APDUs.....	30
96	Figure 8 – GET service with GBT, switching to streaming	32
97	Figure 9 – GET service with partial invocations, GBT and streaming, recovery of 4 th	
98	block sent in the 2nd stream	33
99	Figure 10 – GET service with partial invocations, GBT and streaming, recovery of 4 th	
100	and 5 th block	34
101	Figure 11 – GET service with partial invocations, GBT and streaming, recovery of last	
102	block.....	35
103	Figure 12 – SET service with GBT, with server not supporting streaming, recovery of	
104	3rd block.....	36
105	Figure 13 – ACTION-WITH-LIST service with bi-directional GBT and block recovery	37
106	Figure 14 – DataNotification service with GBT with partial invocation.....	38
107	Figure B. 1 – Short wrapper	43
108		
109	Table 1 – Ciphered xDLMS APDUs	14
110	Table 2 – Use of the fields of the ciphered APDUs	16
111	Table 3 – Security control byte.....	18
112	Table 4 (Replacing Table 7) – HLS example with GMAC	19
113	Table 5 – Additional service parameters	22
114	Table 6 – Security parameters	23
115	Table 7 – Service parameters of the DataNotification service primitives.....	25
116	Table 8 (Replacing Table 31) – Summary of xDLMS services for LN referencing	26
117	Table 9 (Replacing Table 32) – Summary of xDLMS services for SN referencing	26
118	Table 10 (Replacing Table 35) – xDLMS Conformance block	28
119	Table B. 1 – Reserved Application Processes	43
120		
121		

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRICITY METERING DATA EXCHANGE –
THE DLMS/COSEM SUITE –****Part 5-3: DLMS/COSEM application layer – Amendment 1**

FOREWORD

This amendment has been prepared by IEC technical committee 13: Electrical energy measurement and control.

The significant technical changes with respect to IEC 62056-5-3:2013 are listed in Annex G.

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

Revision Report	Report on voting
13/1564/RR	13/XXXX/RVC

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

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

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

ACKNOWLEDGEMENT

Clause 5 is based on parts of NIST documents. Reprinted courtesy of the National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. Not copyrightable in the United States.

The National Committees are requested to note that for this publication the stability date is 2015.

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

158

INTRODUCTION

159

160 This document constitutes Amendment 1 to IEC 62056-5-3:2013, *ELECTRICITY METERING*
161 *DATA EXCHANGE – THE DLMS/COSEM SUITE – Part 5-3: DLMS/COSEM application layer.*

162

ELECTRICITY METERING DATA EXCHANGE – The DLMS/COSEM SUITE –

Part 5-3: DLMS/COSEM application layer – Amendment 1

1 Scope

The text of the Scope of IEC 62056-5-3:2013 as it is.

2 Normative references

Add the following new references to IEC 62056-5-3:2013 Clause 2:

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

NOTE A reference to the undated edition means a reference to the edition 2013 as amended by its Amendment 1.

IEC 62056-5-3:2013, *Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer*

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

IEC 62056-6-2:2013, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*

IEC 62056-6-2:2013 Amd1:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*¹

3 Terms, definitions and abbreviations

3.1 Terms and definitions

The text of IEC 62056-5-3:2013 3.1 as it is.

3.2 Abbreviations

Add the following new abbreviation to IEC 62056-5-3:2013 3.2:

GBT General Block Transfer

4 Overview

4.1 DLMS/COSEM application layer structure

Amend the title as above. Otherwise the text in IEC 62056-5-3:2013 4.1 as it is.

4.2 DLMS/COSEM application layer services

Amend the title as above.

4.2.1 ASO services

The text of IEC 62056-5-3:2013 4.2.1 as it is.

4.2.2 Services provided for application association establishment and release

The text of IEC 62056-5-3:2013 4.2.2 as it is.

¹ To be published simultaneously with this Amendment.

4.2.3 Services provided for data transfer

4.2.3.1 The xDLMS application service element

The text of IEC 62056-5-3:2013 4.2.3.1 with the following amendment:

Replace the sentence below the 5 bullet points:

The additional services are:

- the GET, SET services available to access COSEM object attributes and the ACTION service available to access COSEM object methods using LN referencing, see 4.2.3.5;
- the EventNotification service used by the server to notify the client about events that occur in the server, see 4.2.3.6;
- the DataNotification service used by the server to push data to the client; see 4.2.3.6.

Keep the rest of the text as it is.

4.2.3.2 Client/server and non-client/server type services

The text of IEC 62056-5-3:2013 4.2.3.2 with the following amendment:

Replace the last paragraph:

There are also unsolicited, unconfirmed services. These are requested by the server, on pre-defined conditions, e.g. schedules, triggers or events, to inform the client of the value of one or more attributes, as though they had been requested by the client.

4.2.3.3 Referencing methods and service mapping

The text of IEC 62056-5-3:2013 4.2.3.3 as it is.

4.2.3.4 Confirmed and unconfirmed services

The text of IEC 62056-5-3:2013 4.2.3.4 as it is.

4.2.3.5 DLMS/COSEM client/server type services

Amend the title as above. Otherwise the text of IEC 62056-5-3:2013 4.2.3.5 as it is.

4.2.3.6 Services for event and data notification

Replace the existing title “Services for event notification” as above. Keep the existing text of IEC 62056-5-3:2013 4.2.3.6 and add the following:

To support push operation, the DataNotification service is available. It can be used both in application contexts using SN referencing and LN referencing.

NOTE The DataNotification service is used in conjunction with “Push setup” COSEM interface objects see IEC 62056-6-2:2013 Amd1:— clause 5.3.8.

4.2.3.7 Identifying service invocations: the Invoke_Id parameter

The text of IEC 62056-5-3:2013 4.2.3.7 with the following amendment:

In the DataNotification service – see 6.16 – the Long-Invoke-Id parameter is used instead of the Invoke_Id parameter.

4.2.3.8 Priority of service invocations: the Priority parameter

The text of IEC 62056-5-3:2013 4.2.3.8 as it is.

4.2.3.9 Selective access

The text of IEC 62056-5-3:2013 4.2.3.9 as it is.

4.2.3.10 Multiple references

The text of IEC 62056-5-3:2013 4.2.3.10 as it is.

239 **4.2.3.11 Attribute_0 referencing**240 *The text of IEC 62056-5-3:2013 4.2.3.11 as it is.*241 **4.2.3.12 Transferring long service parameters**242 *Replace the text of IEC 62056-5-3:2013 4.2.3.12 as follows:*243 *Replace the current text with the following:*

244 The COSEM attribute and method related xDLMS service primitives are carried in an encoded
245 form by xDLMS APDUs. This encoded form may be longer than the Client / Server Max
246 Receive PDU Size negotiated. To transfer such 'long' messages, there are two mechanisms
247 available:

248 a) service specific block transfer mechanism: in this case, the service primitive invocations
249 contain only one part – one block – of the data (e.g. attribute values), so that the encoded
250 form fits in a single APDU. Using block transfer with the GET / SET / ACTION (LN
251 referencing) and Read / Write (SN referencing) is a negotiable feature, see 7.3.1;

252 NOTE 1 Block transfer is not available with the unsolicited InformationReport and EventNotification services.

253 NOTE 2 There is no block-recovery mechanism available with these services.

254 b) the general block transfer mechanism specified in 4.2.3.13.

255 The two mechanisms can co-exist.

256 An APDU that fits in the Client / Server Max Receive PDU Size negotiated may be too long to
257 fit in a single frame / packet of the supporting layer. Such APDUs may be transported if the
258 supporting layer provide(s) segmentation; see Annex A.

259 *Add the following new subclause.*

260 **4.2.3.13 The general block transfer mechanism**

261 The general block transfer (GBT) mechanism – supporting also streaming of blocks – can be
262 used with any xDLMS service.

263 NOTE The DataNotification service does not have its own service specific block transfer mechanism. Therefore, to
264 transport long DataNotification APDUs the GBT mechanism is available.

265 With this mechanism, long application layer level messages are carried by General-Block-
266 Transfer APDUs instead of service specific "with-datablock" APDUs.

267 The GBT mechanism supports uni-directional and bi-directional block transfer, streaming and
268 lost block recovery:

269 • uni-directional block transfer means that while one party is sending blocks the other party
270 only confirms the blocks received. If it has blocks to send, it can start sending them when
271 the other party has finished;

272 • bi-directional block transfer means that while one party is sending blocks, the other party
273 not only confirms the blocks received but if it has blocks to send it can send them as well
274 while it is still receiving blocks;

275 NOTE Bi-directional block transfer is useful when long service parameters need to be transported in both
276 directions.

277 • streaming means that several blocks may be sent – streamed – by one party without an
278 acknowledgement of each block from the other party;

279 • lost block recovery means that if the reception of a block is not confirmed, it can be sent
280 again. If streaming is used, lost block recovery takes place at the end of the streaming
281 window.

282 Using the GBT mechanism is a negotiable feature, see 7.3.1.

283 The protocol of the GBT mechanism is specified in 7.3.12.

4.2.4 Layer management services

The text of IEC 62056-5-3:2013 4.2.4 as it is.

4.2.5 Summary of DLMS/COSEM application layer services

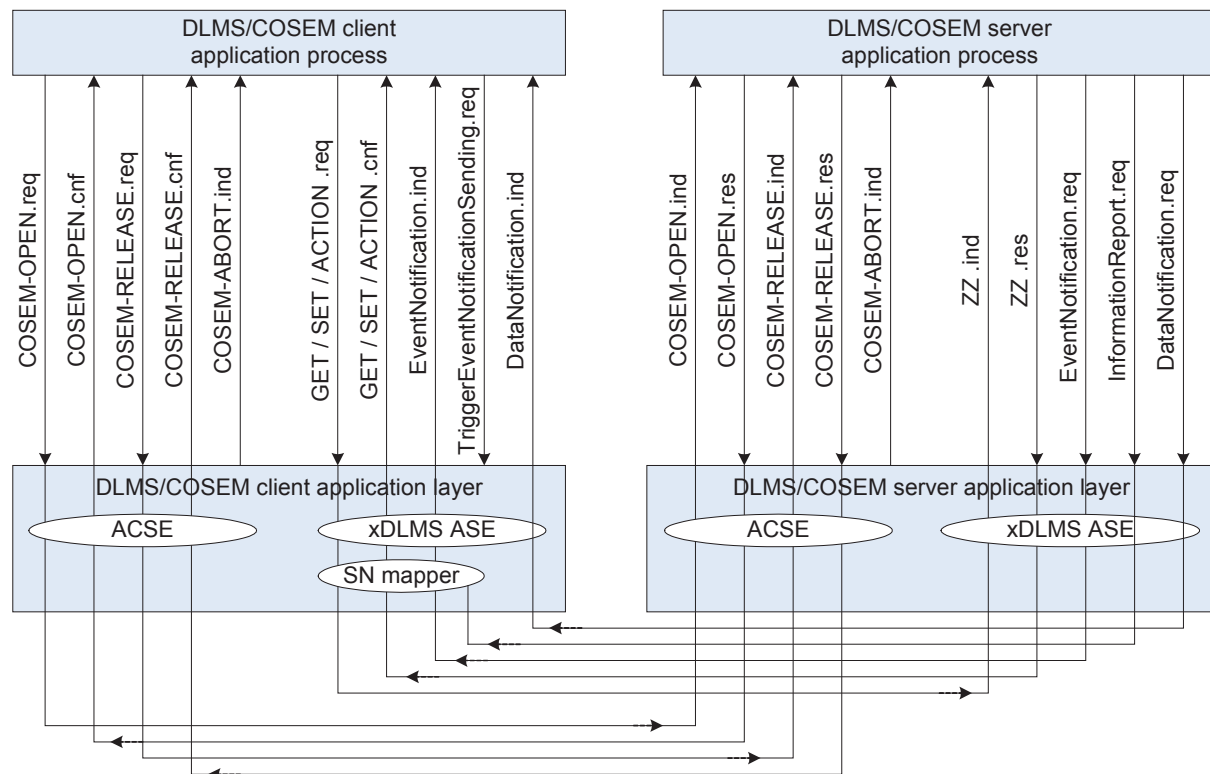
Amend the title as shown above.

The text of IEC 62056-5-3:2013 4.2.4 with the following amendment:

Replace the last sentence of the first paragraph.

The DLMS/COSEM Application layer services are specified in clause 6. The DLMS/COSEM Application layer protocol is specified in clause 7. The abstract syntax of the ACSE and xDLMS APDUs is specified in clause 8. Encoding examples are provided in Annex C, Annex D and Annex E.

Replace Figure 2 with the following Figure 1.



NOTE The client AP always uses LN referencing. If the server uses SN referencing then a mapping is performed by the SN mapper entity of the client AL. Consequently, the service primitives ZZ.ind and ZZ.res may be LN or SN service primitives. LN/SN service mapping is specified in clause 8.

Figure 1 (Replacing Figure 2) – Summary of DLMS/COSEM AL services

4.3 DLMS/COSEM application layer protocols

Amend the title as shown above.

In the text of IEC 62056-5-3:2013 4.3 replace “COSEM AL” by “DLMS/COSEM AL” and “COSEM client” by “DLMS/COSEM client”.

304 5 Information security in DLMS/COSEM

305 *Remove the Note, as it has been included in the Foreword.*

306 5.1 Definitions

307 *The text of IEC 62056-5-3:2013 5.1 as it is.*

308 5.2 General

309 *The text of IEC 62056-5-3:2013 5.2 as it is.*

310 5.3 Data access security

311 5.3.1 Overview

312 *The text of IEC 62056-5-3:2013 5.3.1 as it is.*

313 5.3.2 No security (lowest level security) authentication

314 *Change the title as above. Amend the text to read:*

315 The purpose of No security (lowest level security) authentication is to allow the client to
316 retrieve some basic information from the server. This authentication context does not require
317 any authentication; it allows direct access to the data in the server, within the access rights
318 available in the given AA. The No security authentication mechanism is shown in Figure 2.

319 5.3.3 Low Level Security (LLS) authentication

320 *The text of IEC 62056-5-3:2013 5.3.3 with the following amendment:*

321 *Change the title as above.*

322 *Replace the last sentence to read:*

323 The LLS authentication mechanism is shown in Figure 2.

324 5.3.4 High Level Security (HLS) authentication

325 *The text of IEC 62056-5-3:2013 5.3.4 with the following amendment:*

326 *Change the title as above.*

327 *After Pass 2, add the following:*

328 If StoC is the same as CtoS, the client shall reject it.

329 *In Pass 3, replace the second bullet point by:*

- 330 • in the case of HLS authentication_mechanism_id(3), the client processes StoC
331 concatenating StoC and the shared HLS secret and calculating a digest using the MD5
332 algorithm (RFC 1321):

333
$$f(\text{StoC}) = \text{MD5}(\text{StoC} \parallel \text{HLS secret})$$

334 *In Pass 3, replace the fourth bullet point by:*

- 335 • in the case of HLS authentication_mechanism_id(5), the client processes StoC calculating
336 a hash value T using the GMAC algorithm:

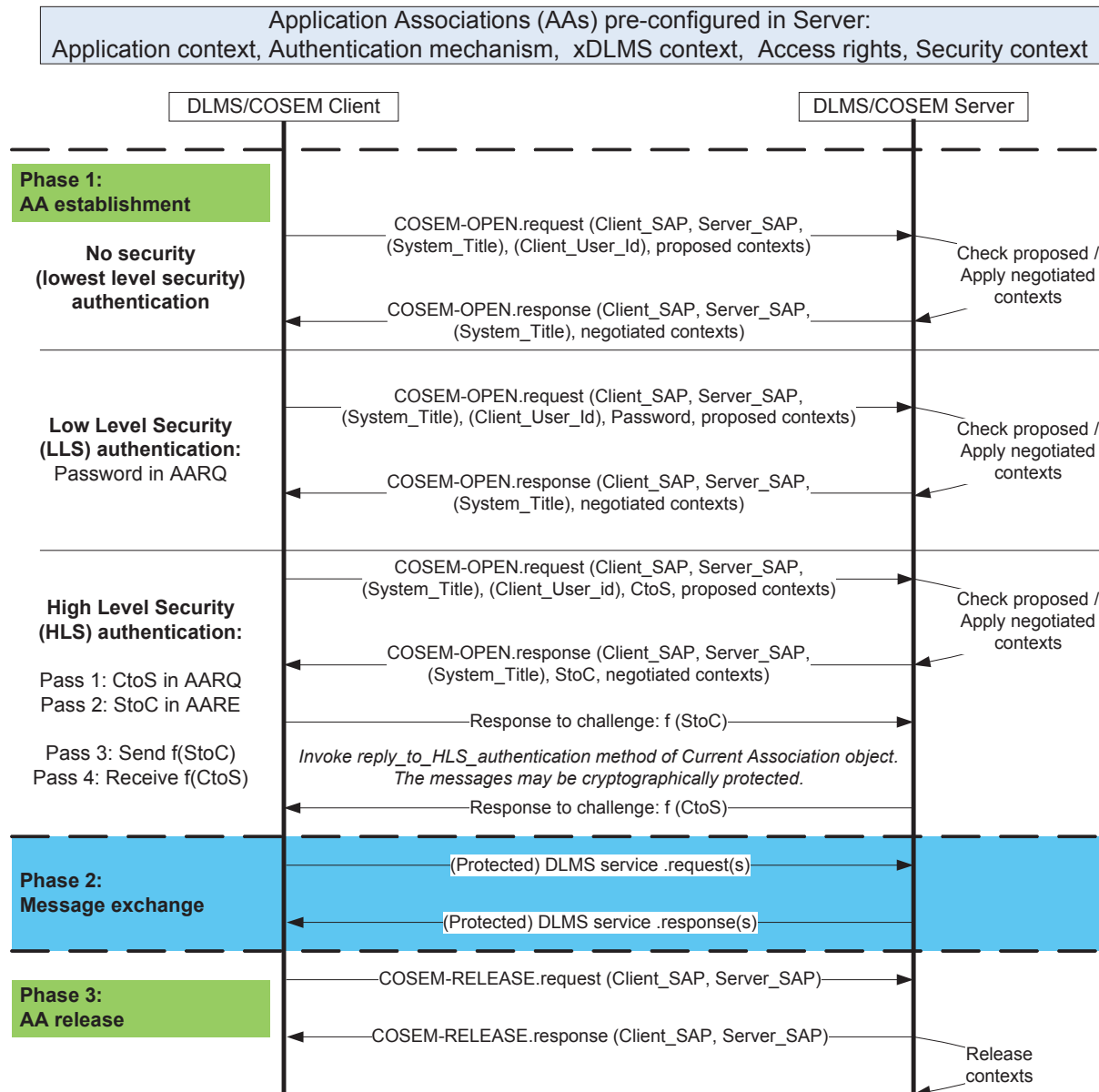
337
$$f(\text{StoC}) = \text{SC} \parallel \text{FC} \parallel \text{T} = \text{SC} \parallel \text{FC} \parallel \text{GMAC}(\text{SC} \parallel \text{AK} \parallel \text{StoC})$$

338 See also 5.4.8.4.

339 *After Pass4, replace the sentence to read:*

340 The HLS authentication mechanism is shown in Figure 2.

341 *Replace IEC 62056-5-3:2013 Figure 3 with the following Figure 2*



NOTE 1 The elements System_Title and Client user (shown in brackets) are optional.

NOTE 2 In pre-established AAs no authentication takes place.

Figure 2 (Replacing Figure 3) – Authentication mechanisms during AA establishment

It is important to note that the security of the message exchange phase is independent of the security of the authentication mechanism. Even in the case where the parties are not authenticated the security of message exchanged can be ensured using cryptographically protected APDUs.

Keep the rest of the text.

5.4 Data transport security**5.4.1 Applying, removing or checking the protection: ciphering and deciphering**

Replace the current text of IEC 62056-5-3:2013 5.4.1 with the following:

xDLMS APDUs – the messages – transported between the client and the server can be protected using cryptographic methods.

NOTE This also applies to the xDLMS Initiate APDUs carried by the AARQ / AARE APDUs.

When a COSEM object attribute or method related xDLMS service primitive is invoked by the AP, the service parameters include the Security_Options parameter. This parameter informs the AL on the kind of ciphered APDU to be used, on the protection to be applied, and includes the necessary security material. The AL builds first the APDU corresponding to the service primitive then it builds the ciphered APDU.

When the AL receives a ciphered APDU, it decipheres it, verifying and removing the protection, restoring the original, unciphered APDU. When this is successfully done, it invokes the appropriate service primitive. The service parameters include the Security_Status parameter, that informs the AP about the kind of ciphered APDU used, on the protection that has been verified and removed, and may include security material. They also include the Protection_Element parameter.

The Security_Options, Security_Status and Protection_Element parameters are specified in 6.5.

Remove Figure 4. A modified version of this Figure is included in 6.5.

5.4.2 Security context

The text of IEC 62056-5-3:2013 5.4.2 as it is.

5.4.3 Security policy

The text of IEC 62056-5-3:2013 5.4.3 as it is.

5.4.4 Security suite

The text of IEC 62056-5-3:2013 5.4.4 as it is.

5.4.5 Security material

The text of IEC 62056-5-3:2013 5.4.5 as it is.

5.4.6 Ciphered xDLMS APDUs

Replace the current text of IEC 62056-5-3:2013 5.4.6 with the following.

Ciphered xDLMS APDUs can be used in a ciphered application context only. In a ciphered application context, unciphered APDUs may also be used.

The different kind of ciphered APDUs are shown in Table 1. Their structure is shown in Figure 3 and Figure 4.

Table 1 – Ciphered xDLMS APDUs

APDU type	Parties	Type of crypto	Security services	Key used
Service specific global / dedicated ciphering	Client – Server	Symmetric	Authentication Encryption	Shared global / dedicated key
general-glo-ciphering				
general-ded-ciphering				

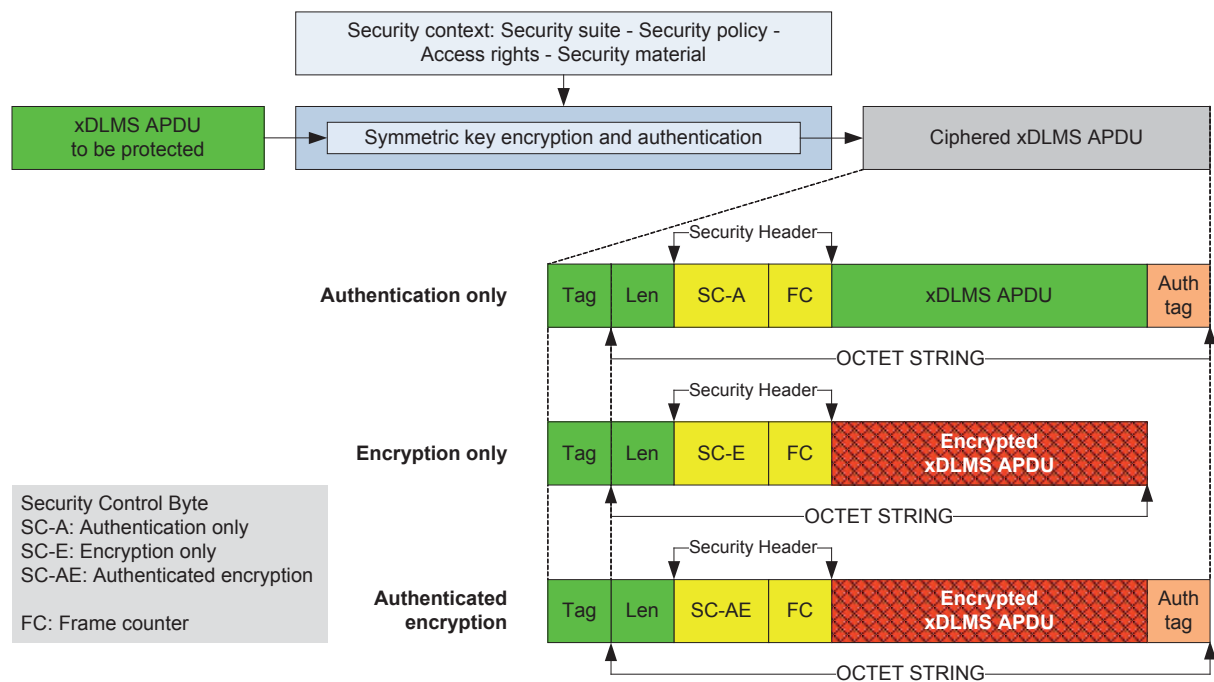
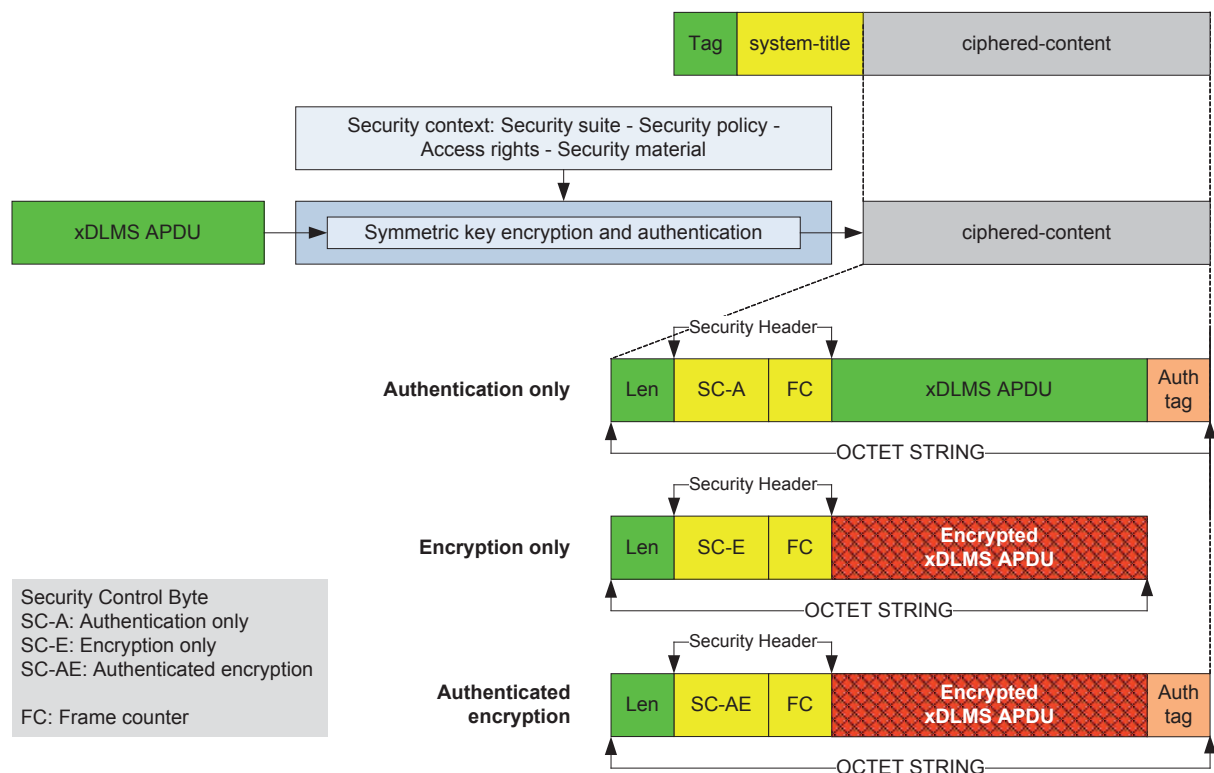


Figure 3 – Structure of service specific global ciphering and dedicated ciphering APDUs



NOTE The purpose to include system-title of the sender is to allow the other party to build the initialization vector where the system-title has not been exchange in another way; see IEC 62056-5-3:2013 5.4.8.3.4.6.

Figure 4 – Structure of general global ciphering and dedicated ciphering APDUs

The use of the fields of the ciphered APDUs is summarized in Table 2.