SLOVENSKI STANDARD
SIST EN IEC 62056-5-3:2024

01-januar-2024

Izmenjava podatkov pri merjenju električne energije - Niz DLMS/COSEM - 5-3. del: Aplikacijska plast DLMS/COSEM (IEC 62056-5-3:2023)

Electrcity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer (IEC 62056-5-3:2023)

Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 5-3: DLMS/COSEM-Anwendungsschicht (IEC 62056-5-3:2023)

Echange des données de comptage de l'électricité - La suite DLMS/COSEM - Partie 5-3: Couche application DLMS/COSEM (IEC 62056-5-3:2023)

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2e-46df-4eae-a497-9ae1e3ff76df/sist-en-iec-62056-5-3-2024

Ta slovenski standard je istoveten z: **EN IEC 62056-5-3:2023**

ICS:

17.220.20	Merjenje električnih in magnetnih veličin	Measurement of electrical and magnetic quantities
35.100.70	Uporabniški sloj	Application layer
91.140.50	Sistemi za oskrbo z elektriko	Electricity supply systems

SIST EN IEC 62056-5-3:2024 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62056-5-3

November 2023

ICS 17.220; 35.110; 91.140.50

Supersedes EN 62056-5-3:2017

English Version

Electricity metering data exchange - The DLMS®/COSEM suite - Part 5-3: DLMS®/COSEM application layer (IEC 62056-5-3:2023)

Échange des données de comptage de l'électricité - La suite DLMS®/COSEM - Partie 5-3: Couche application DLMS®/COSEM
(IEC 62056-5-3:2023)

Datenkommunikation der elektrischen Energiemessung - DLMS®/COSEM - Teil 5-3: DLMS®/COSEM-Anwendungsschicht
(IEC 62056-5-3:2023)

This European Standard was approved by CENELEC on 2023-11-02. 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, Türkiye and the United Kingdom.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

CENELEC

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

© 2023 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62056-5-3:2023 E

SIST EN IEC 62056-5-3:2024

European foreword

The text of document 13/1890/FDIS, future edition 4 of IEC 62056-5-3, 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 62056-5-3:2023.

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) 2024-08-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2026-11-02

This document supersedes EN 62056-5-3:2017 and all of its amendments and corrigenda (if any).

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.

This document has been prepared under a Standardization Request addressed to CENELEC by the European Commission.

Any feedback and questions on this document should be directed to the users’ national committee. A complete listing of these bodies can be found on the CENELEC website.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024

Endorsement notice

The text of the International Standard IEC 62056-5-3:2023 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:

ISO 3166 (series) NOTE Approved as EN ISO 3166 (series)

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.cencenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 61334-4-41	1996	Distribution automation using distribution line carrier systems - Part 4: Data communication protocols - Section 41: Application protocol - Distribution line message specification	EN 61334-4-41	1996
IEC 61334-6	2000	Distribution automation using distribution line carrier systems - Part 6: A-XDR encoding rule	EN 61334-6	2000
IEC/TR 62051	1999	Electricity metering - Glossary of terms	-	-
IEC/TR 62051-1	2004	Electricity metering - Data exchange for meter reading, tariff and load control - Glossary of terms - Part 1: Terms related to data exchange with metering equipment using DLMS®/COSEM	-	-
IEC 62056-6-2	2023	Electricity metering data exchange - The DLMS®/COSEM suite - Part 6-2: COSEM interface classes	EN IEC 62056-6-2	2023
IEC 62056-7-3	2017	Electricity metering data exchange - The DLMS®/COSEM suite - Part 7-3: Wired and wireless M-Bus communication profiles for local and neighbourhood networks	EN 62056-7-3	2017
IEC 62056-7-6	2013	Electricity metering data exchange - The DLMS®/COSEM suite - Part 7-6: The 3-layer, connection-oriented HDLC based communication profile	EN 62056-7-6	2013
IEC 62056-8-3	2013	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-3: Communication profile for PLC S-FSK neighbourhood networks	EN 62056-8-3	2013

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6dd12c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

IEC 62056-8-11	—[1]	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-11: Communication profile for Wi-SUN field area mesh networks	EN IEC 62056-8-11	—[2]
IEC 62056-8-12	2023	Electricity metering data exchange - The DLMS®/COSEM suite - Part 8-12: Communication profile for Low-Power Wide Area Networks (LPWANs)	EN IEC 62056-8-12	2023
IEC 62056-9-7	2013	Electricity metering data exchange - The DLMS/COSEM suite - Part 9-7: Communication profile for TCP-UDP/IP networks	EN 62056-9-7	2013
ISO/IEC 8824-1	2008	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	-	-
ISO/IEC 8825-1	2008	Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	-	-
ISO/IEC 15953	1999	Information technology - Open systems interconnection - Service definition for the Application service object association control service element	-	-
ISO/IEC 15954	1999	Information technology - Open systems interconnection - Connection-mode protocol for the application service object association control service element	-	-
ISO/IEC 7498-1	1994	Information technology - Open Systems Interconnection - Basic reference model: The basic model	-	-
ITU-T X.509	2008	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-
ITU-T X.693	2008	Information technology - ASN.1 encoding rules: XML Encoding rules (XER)	-	-
ITU-T X.693 Corrigendum 1	2011	Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1	-	-
ITU-T X.694	2008	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1	-	-
ITU-T X.694 Corrigendum	2011	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical corrigendum 1	-	-
FIPS PUB 180-4	2012	Secure Hash Standard (SHS)	-	-
FIPS PUB 186-4	2013	Digital Signature Standard (DSS)	-	-

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d0dd12c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

[1] Under preparation. Stage at the time of publication: IEC CDV.

[2] Under preparation. Stage at the time of publication: prEN IEC 62056-8-11:2023.

NIST SP 800-21	2005	Guideline for Implementing Cryptography in the Federal Government	-	-
NIST SP 800-32	2001	Introduction to Public Key Technology and the Federal PKI Infrastructure	-	-
NIST SP 800-56A rev2	2013	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	-	-
NIST SP 800-57	2012	Recommendation for Key Management, Part 1: General (Revision 3)	-	-
NSA2	-	Suite B Implementer's guide to NIST SP800-56A, 28th July 2009	-	-
NSA3	-	NSA Suite B Base Certificate and CRL Profile, 27th May 2008	-	-
SEC1	2009	Standards for Efficient Cryptography: Elliptic Curve Cryptography. SECG. Version 2.0	-	-
RFC 3394	2002	Internet Engineering Task Force (IETF). Advanced Encryption Standard (AES) Key Wrap Algorithm. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories)	-	-
RFC 4106	-	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	-	-
RFC 4108	2005	Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages	-	-
RFC 5280	2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

iTeh Standards
(https://standards.iteh.ai)
Document Preview

SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

IEC 62056-5-3

Edition 4.0 2023-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Échange des données de comptage de l'électricité – La suite DLMS®/COSEM – Partie 5-3: Couche application DLMS®/COSEM

iTeh Standards
(https://standards.iteh.ai)
Document Preview

SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 17.220, 35.110, 91.140.50

ISBN 978-2-8322-7223-7

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 12
INTRODUCTION 14
1 Scope 15
2 Normative references 15
3 Terms, definitions, abbreviated terms and symbols 17
3.1 General DLMS®/COSEM definitions 17
3.2 Definitions related to cryptographic security 22
3.3 Definitions and abbreviated terms related to the Galois/Counter Mode 32
3.4 General abbreviated terms 34
3.5 Symbols related to the Galois/Counter Mode 38
3.6 Symbols related the ECDSA algorithm 38
3.7 Symbols related to the key agreement algorithms 39
4 Overview of DLMS®/COSEM 39
4.1 Information exchange in DLMS®/COSEM 39
4.1.1 General 39
4.1.2 Communication model 40
4.1.3 Naming and addressing 41
4.1.4 Connection oriented operation 44
4.1.5 Application associations 45
4.1.6 Messaging patterns 46
4.1.7 Data exchange between third parties and DLMS®/COSEM servers 47
4.1.8 Communication profiles 48
4.1.9 Model of a DLMS®/COSEM metering system 50
4.1.10 Model of DLMS®/COSEM servers 50
4.1.11 Model of a DLMS®/COSEM client 52
4.1.12 Interoperability and interconnectivity in DLMS®/COSEM 53
4.1.13 Ensuring interconnectivity: the protocol identification service 53
4.1.14 System integration and meter installation 53
4.2 DLMS®/COSEM application layer main features 54
4.2.1 General 54
4.2.2 DLMS®/COSEM application layer structure 54
4.2.3 The Association Control Service Element, ACSE 55
4.2.4 The xDLMS application service element 56
4.2.5 Layer management services 64
4.2.6 Summary of DLMS®/COSEM application layer services 64
4.2.7 DLMS®/COSEM application layer protocols 65
5 Information security in DLMS®/COSEM 65
5.1 Overview 65
5.2 The DLMS®/COSEM security concept 65
5.2.1 Overview 65
5.2.2 Identification and authentication 66
5.2.3 Security context 69
5.2.4 Access rights 69
5.2.5 Application layer message security 69
5.2.6 COSEM data security 72
5.3 Cryptographic algorithms 72

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2e-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

5.3.1 Overview 72
5.3.2 Hash function 72
5.3.3 Symmetric key algorithms 73
5.3.4 Public key algorithms 80
5.3.5 Random number generation 90
5.3.6 Compression 91
5.3.7 Security suite 91
5.4 Cryptographic keys – overview 92
5.5 Key used with symmetric key algorithms 92
5.5.1 Symmetric keys types 92
5.5.2 Key information with general-ciphering APDU and data protection 94
5.5.3 Key identification 94
5.5.4 Key wrapping 95
5.5.5 Key agreement 95
5.5.6 Symmetric key cryptoperiods 96
5.6 Keys used with public key algorithms 96
5.6.1 Overview 96
5.6.2 Key pair generation 96
5.6.3 Public key certificates and infrastructure 97
5.6.4 Certificate and certificate extension profile 100
5.6.5 Suite B end entity certificate types to be supported by DLMS®/COSEM servers 108
5.6.6 Management of certificates 108
5.7 Applying cryptographic protection 113
5.7.1 Overview 113
5.7.2 Protecting xDLMS APDUs 113
5.7.3 Multi-layer protection by multiple parties 126
5.7.4 HLS authentication mechanisms 127
5.7.5 Protecting COSEM data 130
6 DLMS®/COSEM application layer service specification 131
6.1 Service primitives and parameters 131
6.2 The COSEM-OPEN service 133
6.3 The COSEM-RELEASE service 138
6.4 COSEM-ABORT service 141
6.5 Protection and general block transfer parameters 141
6.6 The GET service 146
6.7 The SET service 149
6.8 The ACTION service 153
6.9 The ACCESS service 156
6.9.1 Overview – Main features 156
6.9.2 Service specification 158
6.10 The DataNotification service 162
6.11 The EventNotification service 164
6.12 The TriggerEventNotificationSending service 165
6.13 Variable access specification 166
6.14 The Read service 166
6.15 The Write service 170
6.16 The UnconfirmedWrite service 173
6.17 The InformationReport service 175

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/...-4ede-a497-9ae1e3ff76df/sist-en-iec-62056-5-3-2024

6.18 Client side layer management services: the SetMapperTable.request 176
6.19 Summary of services and LN/SN data transfer service mapping 176
7 DLMS®/COSEM application layer protocol specification 177
7.1 The control function 177
7.1.1 State definitions of the client side control function 177
7.1.2 State definitions of the server side control function 179
7.2 The ACSE services and APDUs 181
7.2.1 ACSE functional units, services and service parameters 181
7.2.2 Registered COSEM names 184
7.2.3 APDU encoding rules 187
7.2.4 Protocol for application association establishment 187
7.2.5 Protocol for application association release 193
7.3 Protocol for the data transfer services 196
7.3.1 Negotiation of services and options – the conformance block 196
7.3.2 Confirmed and unconfirmed service invocations 197
7.3.3 Protocol for the GET service 199
7.3.4 Protocol for the SET service 202
7.3.5 Protocol for the ACTION service 205
7.3.6 Protocol for the ACCESS service 207
7.3.7 Protocol of the DataNotification service 208
7.3.8 Protocol for the EventNotification service 211
7.3.9 Protocol for the Read service 212
7.3.10 Protocol for the Write service 215
7.3.11 Protocol for the UnconfirmedWrite service 219
7.3.12 Protocol for the InformationReport service 220
7.3.13 Protocol of general block transfer mechanism 221
7.3.14 Protocol of exception mechanism 243
8 Abstract syntax of ACSE and COSEM APDUs 244
9 COSEM APDU XML schema 263
9.1 General 263
9.2 XML Schema 263
Annex A (normative) Using the DLMS®/COSEM application layer in various communications profiles 285
A.1 General 285
A.2 Targeted communication environments 285
A.3 The structure of the profile 285
A.4 Identification and addressing schemes 285
A.5 Supporting layer services and service mapping 286
A.6 Communication profile specific parameters of the COSEM AL services 286
A.7 Specific considerations / constraints using certain services within a given profile 286
A.8 The 3-layer, connection-oriented, HDLC based communication profile 286
A.9 The TCP-UDP/IP based communication profiles (COSEM_on_IP) 286
A.10 The wired and wireless M-Bus communication profiles 286
A.11 The S-FSK PLC profile 286
Annex B (normative) SMS short wrapper 287
Annex C (normative) Gateway protocol 288
C.1 General 288
C.2 The gateway protocol 289

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6ddf2c-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

SIST EN IEC 62056-5-3:2024

C.3 HES in the WAN/NN acting as Initiator (Pull operation) 290
C.4 End devices in the LAN acting as Initiators (Push operation) 291
C.4.1 General 291
C.4.2 End device with WAN/NN knowledge 291
C.4.3 End devices without WAN/NN knowledge 291
C.5 Security 291
Annex D (informative) AARQ and AARE encoding examples 292
D.1 General 292
D.2 Encoding of the xDLMS InitiateRequest / InitiateResponse APDU 292
D.3 Specification of the AARQ and AARE APDUs 295
D.4 Data for the examples 296
D.5 Encoding of the AARQ APDU 297
D.6 Encoding of the AARE APDU 300
Annex E (informative) Encoding examples: AARQ and AARE APDUs using a ciphered application context 306
E.1 A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key 306
E.2 Authenticated encryption of the xDLMS InitiateRequest APDU 307
E.3 The AARQ APDU 308
E.4 A-XDR encoding of the xDLMS InitiateResponse APDU 310
E.5 Authenticated encryption of the xDLMS InitiateResponse APDU 311
E.6 The AARE APDU 312
E.7 The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU) 314
E.8 The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU) 315
Annex F (informative) Data transfer service examples 316
F.1 GET / Read, SET / Write examples 316
F.2 ACCESS service example 333
F.3 Compact array encoding example 334
F.3.1 General 334
F.3.2 The specification of compact-array 335
F.3.3 Example 1: Compact array encoding an array of five long-unsigned values 336
F.3.4 Example 2: Compact-array encoding of five octet-string values 337
F.3.5 Example 3: Encoding of the buffer of a Profile generic object 338
F.4 Profile generic IC buffer attribute encoding examples 339
F.4.1 General 339
F.4.2 Get-response with Profile generic normal encoding example 340
F.4.3 Get-response with Profile generic null-data compressed encoding example 342
F.4.4 Get-response with Profile generic compact-array encoding example 345
F.4.5 Get-response with Profile generic null-data and delta-value encoding example 347
F.4.6 Comparison of various encoding methods for Get-response APDU 350
F.4.7 Combination of the various encoding methods and V.44 compression 350
Annex G (normative) NSA Suite B elliptic curves and domain parameters 352
Annex H (informative) Example of an End entity signature certificate using P-256 signed with P-256 354
H.1 Fields of public key certificates 354
H.2 Example of a Root-CA Certificate using P-256 signed with P-256 355

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6d4f7a-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024

SIST EN IEC 62056-5-3:2024

H.3 Example of an end entity digital signature Certificate using P-256 signed with P-256 356
Annex I (normative) Use of key agreement schemes in DLMS®/COSEM 357
I.1 Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme 357
I.2 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme 360
I.3 Static Unified Model C(0e, 2s, ECC CDH) scheme 363
Annex J (informative) Exchanging protected xDLMS APDUs between TP and server 367
J.1 General 367
J.2 Example 1: Protection is the same in the two directions 367
J.3 Example 2: Protection is different in the two directions 368
Annex K (informative) Significant technical changes with respect to IEC 62056-5-3:2017 370
Bibliography 373

Figure 1 – Client–server model and communication protocols 41
Figure 2 – Naming and addressing in DLMS®/COSEM 42
Figure 3 – A complete communication session in the CO environment 44
Figure 4 – DLMS®/COSEM messaging patterns 47
Figure 5 – DLMS®/COSEM generic communication profile 49
Figure 6 – Model of a DLMS®/COSEM metering system 50
Figure 7 – DLMS®/COSEM server model 51
Figure 8 – Model of a DLMS®/COSEM client using multiple protocol stacks 52
Figure 9 – The structure of the DLMS®/COSEM application layers 54
Figure 10 – The concept of composable xDLMS messages 61
Figure 11 – Summary of DLMS®/COSEM AL services 64
Figure 12 – Authentication mechanisms 67
Figure 13 – Client – server message security concept 70
Figure 14 – End-to-end message security concept 71
Figure 15 – Hash function 73
Figure 16 – Encryption and decryption 74
Figure 17 – Message Authentication Codes (MACs) 75
Figure 18 – GCM functions 77
Figure 19 – Digital signatures 83
Figure 20 – C(2e, 0s) scheme: each party contributes only an ephemeral key pair 85
Figure 21 – C(1e, 1s) schemes: party U contributes an ephemeral key pair, and party V contributes a static key pair 86
Figure 22 – C(0e, 2s) scheme: each party contributes only a static key pair 88
Figure 23 – Architecture of a Public Key Infrastructure (example) 99
Figure 24 – MSC for provisioning the server with CA certificates 109
Figure 25 – MSC for security personalisation of the server 110
Figure 26 – Provisioning the server with the certificate of the client 111
Figure 27 – Provisioning the client / third party with a certificate of the server 112
Figure 28 – Remove certificate from the server 112
Figure 29 – Cryptographic protection of information using AES-GCM 116
Figure 30 – Structure of service-specific global / dedicated ciphering xDLMS APDUs 118

iTeh Standards
(https://standards.iteh.ai)
Document Preview
SIST EN IEC 62056-5-3:2024
https://standards.iteh.ai/catalog/standards/sist/5d6dd0f3-46df-4cac-a497-9ae1c3ff76df/sist-en-iec-62056-5-3-2024