IEC 62055-41

Edition 3.0 2018-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Electricity metering – Payment systems – Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0e4659dae/iec-62055-41-2018

Comptage de l'électricité – Systèmes de paiement – Partie 41: Spécification de transfert normalisé (STS) – Protocole de couche application pour les systèmes de supports de jeton unidirectionnel

IEC 62055-41:2018-03(en-fr)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2018 IEC, Geneva, Switzerland

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

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

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

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

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms, containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62455-4:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a6d7-4d7e-9b53-07b0c4639dac/iec-62455-4-2018

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

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

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

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

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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

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

IEC 62055-41

Edition 3.0 2018-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Electricity metering – Payment systems – Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9f5e141-a607-402e-9652-97b0e8520dac/iec-62055-41-2018

Comptage de l'électricité – Systèmes de paiement – Partie 41: Spécification de transfert normalisé (STS) – Protocole de couche application pour les systèmes de supports de jeton unidirectionnel

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 17.220.20; 35.100.70; 91.140.50

ISBN 978-2-8322-5499-8

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 9
INTRODUCTION 11
1 Scope 14
2 Normative references 14
3 Terms, definitions, abbreviated terms, notation and terminology 15
3.1 Terms and definitions 15
3.2 Abbreviated terms 17
3.3 Notation and terminology 19
4 Numbering conventions 19
5 Reference model for the standard transfer specification 20
5.1 Generic payment meter functional reference diagram 20
5.2 STS protocol reference model 21
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier 22
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess 22
5.5 MeterFunctionObjects / companion specifications 24
5.6 Transaction reference numbers 24
6 POSToTokenCarrierInterface application layer protocol 24
6.1 APDU: ApplicationProtocolDataUnit 24
6.1.1 Data elements in the APDU 24
6.1.2 MeterPAN: MeterPrimaryAccountNumber 26
6.1.3 TCT: TokenCarrierType 27
6.1.4 DKGA: DecoderKeyGenerationAlgorithm 28
6.1.5 EA: EncryptionAlgorithm 28
6.1.6 SGC: SupplyGroupCode 28
6.1.7 TI: TariffIndex 29
6.1.8 KRN: KeyRevisionNumber 29
6.1.9 KT: KeyType 29
6.1.10 KEN: KeyExpiryNumber 30
6.1.11 DOE: DateOfExpiry 30
6.1.12 BDT: BaseDate 30
6.2 Tokens 31
6.2.1 Token definition format 31
6.2.2 Class 0: TransferCredit 31
6.2.3 Class 1: InitiateMeterTest/Display 32
6.2.4 Class 2: SetMaximumPowerLimit 32
6.2.5 Class 2: ClearCredit 32
6.2.6 Class 2: SetTariffRate 32
6.2.7 Key change token set for 64-bit DecoderKey transfer 33
6.2.8 Key change token set for 128-bit DecoderKey transfer 34
6.2.9 Class 2: ClearTamperCondition 35
6.2.10 Class 2: SetMaximumPhasePowerUnbalanceLimit 35
6.2.11 Class 2: SetWaterMeterFactor 35
6.2.12 Class 2: Reserved for STS use 35
6.2.13 Class 2: Reserved for Proprietary use 36
6.2.14 Class 3: Reserved for STS use 36
6.3 Token data elements 36

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/0fbe141-a607-402e-9652-07b0c4639dac/iec-62055-41-2018

6.3.1 Data elements used in tokens 36
6.3.2 Class: TokenClass 37
6.3.3 SubClass: TokenSubClass 38
6.3.4 RND: RandomNumber 38
6.3.5 TID: TokenIdentifier 39
6.3.6 Amount: TransferAmount 40
6.3.7 CRC: CyclicRedundancyCheck 44
6.3.8 Control: InitiateMeterTest/DisplayControlField 45
6.3.9 MPL: MaximumPowerLimit 46
6.3.10 MPPUL: MaximumPhasePowerUnbalanceLimit 46
6.3.11 Rate: TariffRate 46
6.3.12 WMFactor: WaterMeterFactor 46
6.3.13 Register: RegisterToClear 46
6.3.14 NKHO: NewKeyHighOrder 46
6.3.15 NKLO: NewKeyLowOrder 46
6.3.16 NKMO1: NewKeyMiddleOrder1 46
6.3.17 NKMO2: NewKeyMiddleOrder2 47
6.3.18 KENHO: KeyExpiryNumberHighOrder 47
6.3.19 KENLO: KeyExpiryNumberLowOrder 47
6.3.20 RO: RolloverKeyChange 47
6.3.21 S&E: SignAndExponent 47
6.3.22 CRC_C: CyclicRedundancyCheck_C 47
6.4 TCDUGeneration functions 47
6.4.1 Definition of the TCDU 47
6.4.2 Transposition of the Class bits 48
6.4.3 TCDUGeneration function for Class 0, 1 and 2 tokens 48
6.4.4 TCDUGeneration function for key change tokens 50
6.4.5 TCDUGeneration function for Set2ndSectionDecoderKey token 51
6.5 Security functions 51
6.5.1 General requirements 51
6.5.2 Key attributes and key changes 51
6.5.3 DecoderKey generation 59
6.5.4 STA: EncryptionAlgorithm07 66
6.5.5 DEA: EncryptionAlgorithm09 69
6.5.6 MISTY1: EncryptionAlgorithm11 69
7 TokenCarriertoMeterInterface application layer protocol 71
7.1 APDU: ApplicationProtocolDataUnit 71
7.1.1 Data elements in the APDU 71
7.1.2 Token 72
7.1.3 AuthenticationResult 72
7.1.4 ValidationResult 72
7.1.5 TokenResult 73
7.2 APDUExtraction functions 74
7.2.1 Extraction process 74
7.2.2 Extraction of the 2 Class bits 74
7.2.3 APDUExtraction function for Class 0 and Class 2 tokens 75
7.2.4 APDUExtraction function for Class 1 tokens 76
7.2.5 APDUExtraction function for key change token set 76
7.3 Security functions 77

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9632-07b0e4659dac/iec-62055-41-2018

7.3.1 Key attributes and key changes 77
7.3.2 DKR: DecoderKeyRegister 77
7.3.3 STA: DecryptionAlgorithm07 78
7.3.4 DEA: DecryptionAlgorithm09 81
7.3.5 MISTY1: DecryptionAlgorithm11 81
7.3.6 TokenAuthentication 83
7.3.7 TokenValidation 83
7.3.8 TokenCancellation 84
8 MeterApplicationProcess requirements 84
8.1 General requirements 84
8.2 Token acceptance/rejection 85
8.3 Display indicators and markings 86
8.4 TransferCredit tokens 86
8.5 InitiateMeterTest/Display tokens 86
8.6 SetMaximumPowerLimit tokens 87
8.7 ClearCredit tokens 87
8.8 SetTariffRate tokens 87
8.9 Key change tokens 87
8.10 Set2ndSectionDecoderKey tokens 88
8.11 ClearTamperCondition tokens 88
8.12 SetMaximumPhasePowerUnbalanceLimit tokens 88
8.13 SetWaterMeterFactor 88
8.14 Class 2: Reserved for STS use tokens 88
8.15 Class 2: Reserved for Proprietary use tokens 88
8.16 Class 3: Reserved for STS use tokens 89
9 KMS: KeyManagementSystem generic requirements 89
10 Maintenance of STS entities and related services 89
10.1 General 89
10.2 Operations 91
10.2.1 Product certification maintenance 91
10.2.2 DSN maintenance 91
10.2.3 RO maintenance 91
10.2.4 TI maintenance 91
10.2.5 TID maintenance 92
10.2.6 SpecialReservedTokenIdentifier maintenance 92
10.2.7 MfrCode maintenance 92
10.2.8 Substitution tables maintenance 92
10.2.9 Permutation tables maintenance 92
10.2.10 SGC maintenance 92
10.2.11 VendingKey maintenance 92
10.2.12 KRN maintenance 92
10.2.13 KT maintenance 92
10.2.14 KEN maintenance 93
10.2.15 CERT maintenance 93
10.2.16 CC maintenance 93
10.2.17 UC maintenance 93
10.2.18 KMCID maintenance 93
10.2.19 CMID maintenance 93
10.3 Standardisation 93

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbc141-a607-402e-9652-
IEC 62055-41:2018

10.3.1 IIN maintenance 93
10.3.2 TCT maintenance 94
10.3.3 DKGA maintenance 94
10.3.4 EA maintenance 94
10.3.5 TokenClass maintenance 94
10.3.6 TokenSubClass maintenance 94
10.3.7 InitiateMeterTest/DisplayControlField maintenance 94
10.3.8 RegisterToClear maintenance 95
10.3.9 STS BaseDate maintenance 95
10.3.10 Rate maintenance 95
10.3.11 WMFactor maintenance 95
10.3.12 MFO maintenance 95
10.3.13 FOIN maintenance 96
10.3.14 Companion specification maintenance 96
Annex A (informative) Guidelines for a KeyManagementSystem (KMS) 97
Annex B (informative) Entities and identifiers in an STS-compliant system 101
Annex C (informative) Code of practice for the implementation of STS-compliant systems 105
C.1 General 105
C.2 Maintenance and support services provided by the STS Association 105
C.3 Key management 105
C.3.1 Key management services 105
C.3.2 SupplyGroupCode and VendingKey distribution 105
C.3.3 CryptographicModule distribution 106
C.3.4 Key expiry 107
C.4 MeterPAN 107
C.4.1 General practice 107
C.4.2 IssuerIdentificationNumbers 107
C.4.3 ManufacturerCodes 107
C.4.4 DecoderSerialNumbers 108
C.5 SpecialReservedTokenIdentifier 108
C.6 Permutation and substitution tables for the STA 108
C.7 EA codes 108
C.8 TokenCarrierType codes 108
C.9 MeterFunctionObject instances / companion specifications 109
C.10 TariffIndex 109
C.11 STS-compliance certification 109
C.11.1 IEC certification services 109
C.11.2 Products 109
C.11.3 Certification authority 109
C.12 Procurement options for users of STS-compliant systems 109
C.13 Management of TID roll over 113
C.13.1 Introduction 113
C.13.2 Overview 114
C.13.3 Impact analysis 115
C.13.4 Base dates 116
C.13.5 Implementation 116
Bibliography 119

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0c4639dac/iec-62055-41-2018

Figure 1 – Functional block diagram of a generic single-device payment meter 20
Figure 2 – STS modelled as a 2-layer collapsed OSI protocol stack 21
Figure 3 – Dataflow from the POSApplicationProcess to the TokenCarrier 22
Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess 23
Figure 5 – Composition of transaction reference number 24
Figure 6 – Transposition of the 2 Class bits 48
Figure 7 – TCDUGeneration function for Class 0, 1 and 2 tokens 49
Figure 8 – TCDUGeneration function for key change tokens 50
Figure 9 – DecoderKey changes – state diagram 57
Figure 10 – DecoderKeyGenerationAlgorithm01 62
Figure 11 – DecoderKeyGenerationAlgorithm02 63
Figure 12 – STA: EncryptionAlgorithm07 66
Figure 13 – STA encryption substitution process 67
Figure 14 – STA encryption permutation process 68
Figure 15 – STA encryption DecoderKey rotation process 68
Figure 16 – STA encryption worked example for TransferCredit token 69
Figure 17 – MISTY1: EncryptionAlgorithm11 70
Figure 18 – MISTY1 encryption worked example for TransferCredit token 71
Figure 19 – APDUExtraction function 74
Figure 20 – Extraction of the 2 Class bits 75
Figure 21 – STA DecryptionAlgorithm07 78
Figure 22 – STA decryption permutation process 78
Figure 23 – STA decryption substitution process 79
Figure 24 – STA decryption DecoderKey rotation process 80
Figure 25 – STA decryption worked example for TransferCredit token 81
Figure 26 – STA DecryptionAlgorithm11 82
Figure 27 – MISTY1 decryption worked example for TransferCredit token 82
Figure A.1 – KeyManagementSystem and interactive relationships between entities 97
Figure B.1 – Entities and identifiers deployed in an STS-compliant system 101
Figure C.1 – System overview 114

Table 1 – Data elements in the APDU 25
Table 2 – Data elements in the IDRecord 25
Table 3 – Data elements in the MeterPAN 26
Table 4 – Data elements in the IAIN / DRN 26
Table 5 – Token carrier types 27
Table 6 – DKGA codes 28
Table 7 – EA codes 28
Table 8 – SGC types and key types 29
Table 9 – DOE codes for the year 30
Table 10 – DOE codes for the month 30
Table 11 – BDT representation 31
Table 12 – Token definition format 31

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0e4679dac/iec-62055-41-2018

Table 13 – Data elements used in tokens 36
Table 14 – Token classes 37
Table 15 – Token sub-classes 38
Table 16 – TID calculation examples 39
Table 17 – Units of measure for electricity 40
Table 18 – Units of measure for other applications 41
Table 19 – Bit allocations for the Amount field for SubClass 0 to 3 41
Table 20 – Maximum error due to rounding 42
Table 21 – Examples of TransferAmount values for credit transfer 42
Table 22 – Bit allocations for the Amount field for SubClass 4 to 7 42
Table 23 – Bit allocations for the exponent e 42
Table 24 – Examples of rounding of negative and positive values 43
Table 25 – Examples of TransferAmounts and rounding errors 44
Table 26 – Example of a CRC calculation 44
Table 27 – Permissible control field values 45
Table 28 – Selection of register to clear 46
Table 29 – S&E bit positions for variables s, e_4, e_3 and e_2 47
Table 30 – Example of a CRC_C calculation 47
Table 31 – Classification of vending keys 53
Table 32 – Classification of decoder keys 53
Table 33 – Permitted relationships between decoder key types 58
Table 34 – Definition of the PANBlock 60
Table 35 – Data elements in the PANBlock 60
Table 36 – Definition of the CONTROLBlock 60
Table 37 – Data elements in the CONTROLBlock 60
Table 38 – Range of applicable decoder reference numbers 61
Table 39 – List of applicable supply group codes 62
Table 40 – Data elements in DataBlock 64
Table 41 – Input parameters for a worked example 65
Table 42 – DataBlock example construction 65
Table 43 – DecoderKey construction example 65
Table 44 – Sample substitution tables 67
Table 45 – Sample permutation table 68
Table 46 – Data elements in the APDU 72
Table 47 – Possible values for the AuthenticationResult 72
Table 48 – Possible values for the ValidationResult 73
Table 49 – Possible values for the TokenResult 73
Table 50 – Values stored in the DKR 77
Table 51 – Sample permutation table 79
Table 52 – Sample substitution tables 80
Table 53 – Entities/services requiring maintenance service 90
Table A.1 – Entities that participate in KMS processes 98
Table A.2 – Processes surrounding the payment meter and DecoderKey 98

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-0700e4059dac/iec-62055-41-2018

Table A.3 – Processes surrounding the CryptographicModule 99
Table A.4 – Processes surrounding the SGC and VendingKey 99
Table B.1 – Typical entities deployed in an STS-compliant system 102
Table B.2 – Identifiers associated with the entities in an STS-compliant system 103
Table C.1 – Data elements associated with a SGC 106
Table C.2 – Data elements associated with the CryptographicModule 107
Table C.3 – Items that should be noted in purchase orders and tenders 110

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0c4639dac/iec-62055-41-2018

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ELECTRICITY METERING – PAYMENT SYSTEMS –

Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0c4639dac/iec-62055-41-2018

International Standard IEC 62055-41 has been prepared by IEC technical committee 13: Electrical energy measurement and control.

This third edition cancels and replaces the second edition of IEC 62055-41, issued in 2014. It constitutes a technical revision.

The main technical changes with regard to the previous edition are as follows:

- currency transfer tokens for electricity, water, gas and time metering;
- finer resolution for gas and time credit transfer;
- common code PAN for 2 and 4 digit manufacturer codes;
- reserved MfrCode values for certification and testing purposes;
- provision for DLMS/COSEM as a virtual token carrier type;

- addition of DKGA04, an advanced key derivation function from 160-bit VendingKey;
- withdrawal of DES for EA09 and TDES for DKGA03 cryptographic algorithms, but DES for DKGA02 remains in use;
- addition of MISTY1 cryptographic algorithm using a 128-bit DecoderKey with supporting key change tokens;
- transfer of SGC values to the meter via key change tokens;
- revision of the test/display token requirements;
- revision of the KMS to reflect current best practice;
- revision of the TID roll over management guidelines;
- definition of BaseDate is referenced to Coordinated Universal Time;
- disassociation of IIN from the ISO standard definition;
- various clarifications and enhancements to support the above.

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

FDIS	Report on voting
13/1755/FDIS	13/1764/RVD

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

A list of all parts in the IEC 62055 series, published under the general title *Electricity metering – Payment systems*, can be found on the IEC website.

IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0c4639dac/iec-62055-41-2018

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

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

INTRODUCTION

The IEC 62055 series covers payment systems, encompassing the customer information systems, point of sale systems, token carriers, payment meters and the respective interfaces that exist between these entities. At the time of preparation of this document, IEC 62055 comprised the following parts, under the general title, *Electricity metering – Payment systems:*

Part 21: Framework for standardization

Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)

Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems

Part 42: Transfer reference numbers (TRN) – Application layer protocol for one-way token carrier systems

Part 51: Standard transfer specification (STS) – Physical layer protocol for one-way numeric and magnetic card token carriers

Part 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection

Part 4x series specify application layer protocols and Part 5x series specify physical layer protocols.

NOTE 1 Part 42 is not interoperable with Part 41, Part 51 and Part 52.

NOTE 2 Part 42 was in preparation at the time of publication of this edition of Part 41.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The standard transfer specification (STS) is a secure message protocol that allows information to be carried between point of sale (POS) equipment and payment meters and it caters for several message types such as credit, configuration control, display and test instructions. It further specifies devices and codes of practice that allow for the secure management (generation, storage, retrieval and transportation) of cryptographic keys used within the system.

IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-403e-9652-07b0c4639dac/iec-62055-41-2018

The token carrier, which is not specified in this part of IEC 62055, is the physical device or medium used to transport the information from the POS equipment to the payment meter. Three types of token carriers are currently specified in IEC 62055-51 and IEC 62055-52; the magnetic card, the numeric token carrier and a virtual token carrier, which have been approved by the STS Association. New token carriers can be proposed as new work items through the National Committees or through the STS Association.

Although the main implementation of the STS is in the electricity supply industry, it inherently provides for the management of other utility services such as water and gas. It should be noted that certain functionalities may not apply across all utility services, for example, MaximumPowerLimit in the case of a water meter. Similarly, certain terminology may not be appropriate in non-electrical applications, for example, Load Switch in the case of a gas meter. Future revisions of the STS may allow for other token carrier technologies like smart cards and memory keys with two-way functionality and to cater for a real-time clock and complex tariffs in the payment meter.

Not all the requirements specified in this document are compulsory for implementation in a particular system configuration and as a guideline, a selection of optional configuration parameters are listed in Clause C.12.

The STS Association is registered with the IEC as a Registration Authority for providing maintenance services in support of the STS (see Clause C.1 for more information).

Publication of the first edition of IEC 62055-41 in May 2007 resulted in its rapid adoption as the preferred global standard for prepayment meters in many IEC member countries and a

majority of IEC affiliate member countries. Prepayment electricity meters and their associated Payment Systems are now produced, operated and maintained by an ecosystem of utilities, meter manufacturers, meter operators, vending system providers, vending agents, banking institutions and adjacent industries. Multi-stakeholder interests are served by the STS Association comprising of more than 150 organisations located in over 35 countries. Interoperability and conformance to the Standard Transfer Specification (STS) are guaranteed by Conformance test specifications developed and administered by the STS Association. A full list of the STS Association services can be found at http://www.sts.org.za.

Developed originally for prepayment electricity meters in Africa – via an IEC TC13 WG15 D-type liaison with the STS Association – this IEC standard now serves more users in Asia than Africa, with a total of approximately 50 million meters operated by 500 utilities in 94 countries. Management of the technology has been administered by the STS Association in fulfilment of its role as the IEC appointed Registration Authority.

With the ongoing development of advanced cryptographic algorithms, it has become desirable to revise the security levels of IEC 62055-41 so as to reflect the state of the art best practices, which will be appropriate for deployment of new systems having a useful life expectancy of at least the next 30 years.

Similarly, smart metering systems with payment functionality have evolved to employ tariff functions in the meter, thus raising the need to provide for the transfer of currency units to the meter instead of service units.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning special reserved token identifier given in 6.3.5.2.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

IEC takes no position concerning the evidence, validity and scope of this patent right.

IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-97b0a4629dad/iec-62055-41-2018

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from:

Address:	Itron Measurement and Systems, P.O. Box 4059,TygerValley 7536, Republic of South Africa
Tel:	+27 21 928 1700
Fax:	+27 21 928 1701
Website:	http://www.itron.com

Address:	Conlog (Pty) Ltd, P.O. Box 2332, Durban 4000, Republic of South Africa
Tel:	+27 31 2681141
Fax:	+27 31 2087790
Website:	http://www.conlog.co.za

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a

maintenance service concerning encryption key management and the stack of protocols on which the present International Standard IEC 62055-41 is based [see Clause C.1]. The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the IEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the IEC. Information may be obtained from:

Address:	The STS Association, P.O. Box 868, Ferndale 2160, Republic of South Africa
Tel:	+27 11 061 5000
Fax:	+27 86 679 4500
Email:	support@sts.org.za
Website:	http://www.sts.org.za

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62055-41:2018
https://standards.iteh.ai/catalog/standards/sist/a9fbe141-a607-402e-9652-07b0c4639dac/iec-62055-41-2018