IEC 62055-41

Edition 3.0 2018-03

REDLINE VERSION

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 17.220.20; 35.100.70; 91.140.50

ISBN 978-2-8322-5556-8

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 9
INTRODUCTION 2
1 Scope 15
2 Normative references 15
3 Terms, definitions, abbreviated terms, notation and terminology 15
3.1 Terms and definitions 16
3.2 Abbreviated terms 18
3.3 Notation and terminology 18
4 Numbering conventions 20
5 Reference model for the standard transfer specification 21
5.1 Generic payment meter functional reference diagram 21
5.2 STS protocol reference model 21
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier 23
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess 23
5.5 MeterFunctionObjects / companion specifications 24
5.6 ~~ISO~~ Transaction reference numbers 25
6 POSToTokenCarrierInterface application layer protocol 25
6.1 APDU: ApplicationProtocolDataUnit 25
6.1.1 Data elements in the APDU 25
6.1.2 MeterPAN: MeterPrimaryAccountNumber 27
6.1.3 TCT: TokenCarrierType 28
6.1.4 DKGA: DecoderKeyGenerationAlgorithm 29
6.1.5 EA: EncryptionAlgorithm 29
6.1.6 SGC: SupplyGroupCode 30
6.1.7 TI: TariffIndex 31
6.1.8 KRN: KeyRevisionNumber 31
6.1.9 KT: KeyType 31
6.1.10 KEN: KeyExpiryNumber 31
6.1.11 DOE: DateOfExpiry 31
6.1.12 BDT: BaseDate 32
6.2 Tokens 32
6.2.1 Token definition format 32
6.2.2 Class 0: TransferCredit 33
6.2.3 Class 1: InitiateMeterTest/Display 33
6.2.4 Class 2: SetMaximumPowerLimit 34
6.2.5 Class 2: ClearCredit 34
6.2.6 Class 2: SetTariffRate 34
6.2.7 Key change token set for 64-bit DecoderKey transfer 34
6.2.8 Key change token set for 128-bit DecoderKey transfer 35
6.2.9 Class 2: ClearTamperCondition 36
6.2.10 Class 2: SetMaximumPhasePowerUnbalanceLimit 37
6.2.11 Class 2: SetWaterMeterFactor 37
6.2.12 Class 2: Reserved for STS use 37
6.2.13 Class 2: Reserved for Proprietary use 37
6.2.14 Class 3: Reserved for STS use 37
6.3 Token data elements 34

6.3.1 Data elements used in tokens 38
6.3.2 Class: TokenClass 39
6.3.3 SubClass: TokenSubClass 40
6.3.4 RND: RandomNumber 40
6.3.5 TID: TokenIdentifier 41
6.3.6 Amount: TransferAmount 43
6.3.7 CRC: CyclicRedundanc~~Code~~Check 46
6.3.8 Control: InitiateMeterTest/DisplayControlField 46
6.3.9 MPL: MaximumPowerLimit 47
6.3.10 MPPUL: MaximumPhasePowerUnbalanceLimit 48
6.3.11 Rate: TariffRate 48
6.3.12 WMFactor: WaterMeterFactor 48
6.3.13 Register: RegisterToClear 48
6.3.14 NKHO: NewKeyHighOrder 48
6.3.15 NKLO: NewKeyLowOrder 48
6.3.16 NKMO1: NewKeyMiddleOrder1 48
6.3.17 NKMO2: NewKeyMiddleOrder2 48
6.3.18 KENHO: KeyExpiryNumberHighOrder 49
6.3.19 KENLO: KeyExpiryNumberLowOrder 49
6.3.20 RO: RolloverKeyChange 49
6.3.21 S&E: SignAndExponent 49
6.3.22 CRC_C: CyclicRedundancyCheck_C 49
6.4 TCDUGeneration functions 49
6.4.1 Definition of the TCDU 49
6.4.2 Transposition of the Class bits 49
6.4.3 TCDUGeneration function for Class 0,1 and 2 tokens 50
6.4.4 TCDUGeneration function for ~~Set1stSectionDecoderKey~~ key change tokens 52
6.4.5 TCDUGeneration function for Set2ndSectionDecoderKey token 54
6.5 Security functions 54
6.5.1 General requirements 55
6.5.2 Key attributes and key changes 55
6.5.3 DecoderKey generation 64
6.5.4 STA: EncryptionAlgorithm07 69
6.5.5 DEA: EncryptionAlgorithm09 75
6.5.6 MISTY1: EncryptionAlgorithm11 75
7 TokenCarriertoMeterInterface application layer protocol 75
7.1 APDU: ApplicationProtocolDataUnit 77
7.1.1 Data elements in the APDU 77
7.1.2 Token 78
7.1.3 AuthenticationResult 78
7.1.4 ValidationResult 78
7.1.5 TokenResult 79
7.2 APDUExtraction functions 80
7.2.1 Extraction process 80
7.2.2 Extraction of the 2 Class bits 80
7.2.3 APDUExtraction function for Class 0 and Class 2 tokens 81
7.2.4 APDUExtraction function for Class 1 tokens 82

7.2.5 APDUExtraction function for ~~Set1stSectionDecoderKey and Set2ndSectionDecoderKey~~ key change token~~s~~ set 82
7.3 Security functions 83
7.3.1 Key attributes and key changes 83
7.3.2 DKR: DecoderKeyRegister 83
7.3.3 STA: DecryptionAlgorithm07 84
7.3.4 DEA: DecryptionAlgorithm09 87
7.3.5 MISTY1: DecryptionAlgorithm11 88
7.3.6 TokenAuthentication 87
7.3.7 TokenValidation 90
7.3.8 TokenCancellation 90
8 MeterApplicationProcess requirements 91
8.1 General requirements 91
8.2 Token acceptance/rejection 91
8.3 Display indicators and markings 92
8.4 TransferCredit tokens 93
8.5 InitiateMeterTest/Display tokens 93
8.6 SetMaximumPowerLimit tokens 94
8.7 ClearCredit tokens 94
8.8 SetTariffRate tokens 94
8.9 ~~Set1stSectionDecoderKey~~ Key change tokens 94
8.10 Set2ndSectionDecoderKey tokens 95
8.11 ClearTamperCondition tokens 95
8.12 SetMaximumPhasePowerUnbalanceLimit tokens 95
8.13 SetWaterMeterFactor 95
8.14 Class 2: Reserved for STS use tokens 95
8.15 Class 2: Reserved for Proprietary use tokens 95
8.16 Class 3: Reserved for STS use tokens 95
9 KMS: KeyManagementSystem generic requirements 96
10 Maintenance of STS entities and related services 96
10.1 General 96
10.2 Operations 98
10.2.1 Product certification maintenance 98
10.2.2 DSN maintenance 98
10.2.3 RO maintenance 98
10.2.4 TI maintenance 98
10.2.5 TID maintenance 99
10.2.6 SpecialReservedTokenIdentifier maintenance 99
10.2.7 MfrCode maintenance 99
10.2.8 Substitution tables maintenance 99
10.2.9 Permutation tables maintenance 99
10.2.10 SGC maintenance 99
10.2.11 VendingKey maintenance 99
10.2.12 KRN maintenance 99
10.2.13 KT maintenance 99
10.2.14 KEN maintenance 100
10.2.15 ~~KEK~~ CERT maintenance 100
10.2.16 CC maintenance 100
10.2.17 UC maintenance 100

10.2.18 KMCID maintenance 100
10.2.19 CMID maintenance 100
~~CMAC maintenance~~ .....
10.3 Standardisation 100
10.3.1 IIN maintenance 101
10.3.2 TCT maintenance 101
10.3.3 DKGA maintenance 101
10.3.4 EA maintenance 101
10.3.5 TokenClass maintenance 101
10.3.6 TokenSubClass maintenance 102
10.3.7 InitiateMeterTest/DisplayControlField maintenance 102
10.3.8 RegisterToClear maintenance 102
10.3.9 STS BaseDate maintenance 102
10.3.10 Rate maintenance 102
10.3.11 WMFactor maintenance 102
10.3.12 MFO maintenance 103
10.3.13 FOIN maintenance 103
10.3.14 Companion specification maintenance 103
Annex A (informative) Guidelines for a KeyManagementSystem (KMS) 104
Annex B (informative) Entities and identifiers in an STS-compliant system 108
Annex C (informative) Code of practice for the implementation of STS-compliant systems 112
C.1 General 112
C.2 Maintenance and support services provided by the STS Association 112
C.3 Key management 112
C.3.1 Key management services 112
C.3.2 SupplyGroupCode and VendingKey distribution 112
C.3.3 CryptographicModule distribution 113
C.3.4 Key expiry 114
C.4 MeterPAN 114
C.4.1 General practice 114
C.4.2 IssuerIdentificationNumbers 114
C.4.3 ManufacturerCodes 114
C.4.4 DecoderSerialNumbers 115
C.5 SpecialReservedTokenIdentifier 115
C.6 Permutation and substitution tables for the STA 115
C.7 EA codes 115
C.8 TokenCarrierType codes 115
C.9 MeterFunctionObject instances / companion specifications 116
C.10 TariffIndex 116
C.11 STS-compliance certification 116
C.11.1 IEC certification services 116
C.11.2 Products 116
C.11.3 Certification authority 116
C.12 Procurement options for users of STS-compliant systems 117
C.13 Management of TID roll over 120
C.13.1 Introduction 120
C.13.2 Overview 121
C.13.3 Impact analysis 123

C.13.4 Base dates 124
C.13.5 Implementation 124
Bibliography 127

~~Figure – TCDUGeneration function for Set2ndSectionDecoderKey token .....~~
~~Figure – DecoderKeyGenerationAlgorithm03 .....~~
~~Figure – DEA: EncryptionAlgorithm09 .....~~
~~Figure – DEA DecryptionAlgorithm09 .....~~
Figure 1 – Functional block diagram of a generic single-~~part~~ device payment meter 21
Figure 2 – STS modelled as a 2-layer collapsed OSI protocol stack 22
Figure 3 – Dataflow from the POSApplicationProcess to the TokenCarrier 23
Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess 24
Figure 5 – ~~ISO~~ Composition of transaction reference number 25
Figure 6 – Transposition of the 2 Class bits 50
Figure 7 – TCDUGeneration function for Class 0, 1 and 2 tokens 51
Figure 8 – TCDUGeneration function for key change tokens 52
Figure 9 – DecoderKey changes – state diagram 61
Figure 10 – DecoderKeyGenerationAlgorithm01 67
Figure 11 – DecoderKeyGenerationAlgorithm02 68
Figure 12 – STA: EncryptionAlgorithm07 71
Figure 13 – STA encryption substitution process 72
Figure 14 – STA encryption permutation process 73
Figure 15 – STA encryption DecoderKey rotation process 73
Figure 16 – STA encryption worked example for TransferCredit token 74
Figure 17 – MISTY1: EncryptionAlgorithm11 76
Figure 18 – MISTY1 encryption worked example for TransferCredit token 77
Figure 19 – APDUExtraction function 80
Figure 20 – Extraction of the 2 Class bits 81
Figure 21 – STA DecryptionAlgorithm07 84
Figure 22 – STA decryption permutation process 84
Figure 23 – STA decryption substitution process 85
Figure 24 – STA decryption DecoderKey rotation process 86
Figure 25 – STA decryption worked example for TransferCredit token 87
Figure 26 – STA DecryptionAlgorithm11 88
Figure 27 – MISTY1 decryption worked example for TransferCredit token 89
Figure A.1 – KeyManagementSystem and interactive relationships between entities 104
Figure B.1 – Entities and identifiers deployed in an STS-compliant system 108
Figure C.1 – System overview 122

Table 1 – Data elements in the APDU 26
Table 2 – Data elements in the IDRecord 26
Table 3 – Data elements in the MeterPAN 27
Table 4 – Data elements in the IAIN / DRN 28

Table 5 – Token carrier types 29
Table 6 – DKGA codes 29
Table 7 – EA codes 30
Table 8 – SGC types and key types 30
Table 9 – DOE codes for the year 32
Table 10 – DOE codes for the month 32
Table 11 – BDT representation 32
Table 12 – Token definition format 33
Table 13 – Data elements used in tokens 38
Table 14 – Token classes 39
Table 15 – Token sub-classes 40
Table 16 – TID calculation examples 42
Table 17 – Units of measure for electricity 43
Table 18 – Units of measure for other applications 43
Table 19 – Bit allocations for the ~~Transfer~~ Amount field for SubClass 0 to 3 43
Table 20 – Maximum error due to rounding 44
Table 21 – Examples of TransferAmount values for credit transfer 44
Table 22 – Bit allocations for the Amount field for SubClass 4 to 7 44
Table 23 – Bit allocations for the exponent e 45
Table 24 – Examples of rounding of negative and positive values 45
Table 25 – Examples of TransferAmounts and rounding errors 46
Table 26 – Example of a CRC calculation 46
Table 27 – Permissible control field values 47
Table 28 – Selection of register to clear 48
Table 29 – S&E bit positions for variables s, e_4, e_3 and e_2 49
Table 30 – Example of a CRC_C calculation 49
Table 31 – Classification of vending keys 57
Table 32 – Classification of decoder keys 57
Table 33 – Permitted relationships between decoder key types 62
Table 34 – Definition of the PANBlock 64
Table 35 – Data elements in the PANBlock 64
Table 36 – Definition of the CONTROLBlock 65
Table 37 – Data elements in the CONTROLBlock 65
Table 38 – Range of applicable decoder reference numbers 66
Table 39 – List of applicable supply group codes 66
Table 40 – Data elements in DataBlock 70
Table 41 – Input parameters for a worked example 70
Table 42 – DataBlock example construction 71
Table 43 – DecoderKey construction example 71
Table 44 – Sample substitution tables 72
Table 45 – Sample permutation table 73
Table 46 – Data elements in the APDU 78
Table 47 – Possible values for the AuthenticationResult 78

Table 48 – Possible values for the ValidationResult 79
Table 49 – Possible values for the TokenResult 79
Table 50 – Values stored in the DKR 83
Table 51 – Sample permutation table 85
Table 52 – Sample substitution tables 86
Table 53 – Entities/services requiring maintenance service 97
Table A.1 – Entities that participate in KMS processes 105
Table A.2 – Processes surrounding the payment meter and DecoderKey 105
Table A.3 – Processes surrounding the CryptographicModule 106
Table A.4 – Processes surrounding the SGC and VendingKey 106
Table B.1 – Typical entities deployed in an STS-compliant system 109
Table B.2 – Identifiers associated with the entities in an STS-compliant system 110
Table C.1 – Data elements associated with a SGC 113
Table C.2 – Data elements associated with the CryptographicModule 114
Table C.3 – Items that should be noted in purchase orders and tenders 117

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.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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.

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.

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

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

IMPORTANT – The "colour inside" logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

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.

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.

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 ~~130~~ 150 organisations located in over ~~24~~ 35 countries. Interoperability and conformance to the Standard Transfer ~~System~~ 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 ~~35~~ 50 million meters operated by ~~400~~ 500 utilities in ~~30~~ 94 countries. Management of the technology has been administered by the STS Association in fulfilment of its role as the IEC appointed Registration Authority.

~~Global success has brought about an urgent need to extend the range of the numerical elements contained in IEC 62055-41 tables. In particular, the range of manufacturer numbers need to be extended beyond the 99 numbers originally provided. Also, application of the standard has been extended to cater for multi-energy systems including gas and water meters. Accordingly, there is a need to ensure that the content of IEC 62055-41 is maintained to cater for this market growth and multi-energy extensions.~~

~~Several corrections and clarifications are also required to bring Ed 1 up to date with current practice. This was considered by TC13 WG15 at its meeting on the 20 September 2012 in London, where it was agreed that IEC 62055-41 should be revised.~~

~~Only the most urgently required revisions have been incorporated in Edition 2 due to timing constraints, but it is anticipated that Edition 3 will consider further revisions to incorporate the following functionalities:~~

- ~~Currency transfer~~
- ~~Enhanced security on par with contemporary industry practice~~
- ~~Complex functions fully harmonized with DLMS/COSEM suite~~
- ~~Decentralized key management system with distributed architecture~~
- ~~Conformance certification test suite in conjunction with IECEE CB scheme~~

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.

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

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

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

1 Scope

This part of IEC 62055 specifies the application layer protocol of the STS for transferring units of credit and other management information from a point of sale (POS) system to an STS-compliant payment meter in a one-way token carrier system. It is primarily intended for application with electricity payment meters without a tariff employing energy-based tokens, but may also have application with currency-based token systems and for services other than electricity.

It specifies:

- a POS to token carrier interface structured with an application layer protocol and a physical layer protocol using the OSI model as reference;
- tokens for the application layer protocol to transfer the various messages from the POS to the payment meter;
- security functions and processes in the application layer protocol such as the Standard Transfer Algorithm and the Data Encryption Algorithm, including the generation and distribution of the associated cryptographic keys;
- security functions and processes in the application layer protocol at the payment meter such as decryption algorithms, token authentication, validation and cancellation;
- specific requirements for the meter application process in response to tokens received;
- a scheme for dealing with payment meter functionality in the meter application process and associated companion specifications;
- generic requirements for an STS-compliant key management system;
- guidelines for a key management system;
- entities and identifiers used in an STS system;
- code of practice for the management of TID roll-over key changes in association with the revised set of base dates;
- code of practice and maintenance support services from the STS Association.

It is intended for use by manufacturers of payment meters that have to accept tokens that comply with the STS and also by manufacturers of POS systems that have to produce STS-compliant tokens and is to be read in conjunction with IEC 62055-5x series.

STS-compliant products are required to comply with selective parts of this document only, which is the subject of the purchase contract (see also Clause C.12).

NOTE Although developed for payment systems for electricity, the document also makes provision for tokens used in other utility services, such as water and gas.

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 60050 (all parts), *International Electrotechnical Vocabulary (available at <http://www.electropedia.org>)*~~

IEC TR 62051:1999, *Electricity metering – Glossary of terms*

IEC TR 62055-21:2005, *Electricity metering – Payment systems – Part 21: Framework for standardization*

IEC 62055-31:2005, *Electricity metering – Payment systems – Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)*

IEC 62055-51:2007, *Electricity metering – Payment systems – Part 51: Standard transfer specification (STS) – Physical layer protocol for one-way numeric and magnetic card token carriers*

IEC 62055-52:2008, *Electricity metering – Payment systems – Part 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection*

ISO/IEC 7812-1:~~2006~~ 2017, *Identification cards – Identification of issuers – Part 1: Numbering system*

~~ISO/IEC 7812-2:2007, *Identification cards – Identification of issuers – Part 2: Application and registration procedures*~~

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers*

ISO 9797-2, *Information technology – Security techniques – Message Authentication. Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO 10118-3, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated Hash Functions*

ANSI X3.92-1981, *American National Standard Data Encryption Algorithm, American National Standards Institute – Data Encryption Algorithm*

FIPS PUB 46-3:1999, *Federal Information Processing Standards Publication – Data Encryption Standard*

NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*

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

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)

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

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

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

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

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

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

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

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.

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.

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.

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.

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.

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.

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

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

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

1 Scope

This part of IEC 62055 specifies the application layer protocol of the STS for transferring units of credit and other management information from a point of sale (POS) system to an STS-compliant payment meter in a one-way token carrier system. It is primarily intended for application with electricity payment meters without a tariff employing energy-based tokens, but may also have application with currency-based token systems and for services other than electricity.

It specifies:

- a POS to token carrier interface structured with an application layer protocol and a physical layer protocol using the OSI model as reference;
- tokens for the application layer protocol to transfer the various messages from the POS to the payment meter;
- security functions and processes in the application layer protocol such as the Standard Transfer Algorithm and the Data Encryption Algorithm, including the generation and distribution of the associated cryptographic keys;
- security functions and processes in the application layer protocol at the payment meter such as decryption algorithms, token authentication, validation and cancellation;
- specific requirements for the meter application process in response to tokens received;
- a scheme for dealing with payment meter functionality in the meter application process and associated companion specifications;
- generic requirements for an STS-compliant key management system;
- guidelines for a key management system;
- entities and identifiers used in an STS system;
- code of practice for the management of TID roll-over key changes in association with the revised set of base dates;
- code of practice and maintenance support services from the STS Association.

It is intended for use by manufacturers of payment meters that have to accept tokens that comply with the STS and also by manufacturers of POS systems that have to produce STS-compliant tokens and is to be read in conjunction with IEC 62055-5x series.

STS-compliant products are required to comply with selective parts of this document only, which is the subject of the purchase contract (see also Clause C.12).

NOTE Although developed for payment systems for electricity, the document also makes provision for tokens used in other utility services, such as water and gas.

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 TR 62051:1999, *Electricity metering – Glossary of terms*

IEC TR 62055-21:2005, *Electricity metering – Payment systems – Part 21: Framework for standardization*

IEC 62055-31:2005, *Electricity metering – Payment systems – Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)*

IEC 62055-51:2007, *Electricity metering – Payment systems – Part 51: Standard transfer specification (STS) – Physical layer protocol for one-way numeric and magnetic card token carriers*

IEC 62055-52:2008, *Electricity metering – Payment systems – Part 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection*

ISO/IEC 7812-1:2017, *Identification cards – Identification of issuers – Part 1: Numbering system*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers*

ISO 9797-2, *Information technology – Security techniques – Message Authentication. Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO 10118-3, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated Hash Functions*

ANSI X3.92-1981, *American National Standard Data Encryption Algorithm, American National Standards Institute – Data Encryption Algorithm*

FIPS PUB 46-3:1999, *Federal Information Processing Standards Publication – Data Encryption Standard*

NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*

SOMMAIRE

AVANT-PROPOS 129
INTRODUCTION 131
1 Domaine d'application 134
2 Références normatives 135
3 Termes, définitions, termes abrégés, notation et terminologie 135
3.1 Termes et définitions 135
3.2 Termes abrégés 137
3.3 Notation et terminologie 139
4 Conventions de numérotation 140
5 Modèle de référence pour la spécification de transfert normalisé 141
5.1 Diagramme fonctionnel de référence pour compteur à paiement générique 141
5.2 Modèle de référence de protocole STS 143
5.3 Flux de données du POSApplicationProcess vers le TokenCarrier 144
5.4 Flux de données du TokenCarrier vers le MeterApplicationProcess 145
5.5 MeterFunctionObjects / spécifications d'accompagnement 146
5.6 Numéros de référence des transactions 147
6 Protocole de couche application POSToTokenCarrierInterface 148
6.1 APDU: ApplicationProtocolDataUnit 148
6.1.1 Éléments de données dans l'APDU 148
6.1.2 MeterPAN: MeterPrimaryAccountNumber 149
6.1.3 TCT: TokenCarrierType 151
6.1.4 DKGA: DecoderKeyGenerationAlgorithm 151
6.1.5 EA: EncryptionAlgorithm 152
6.1.6 SGC: SupplyGroupCode 152
6.1.7 TI: TariffIndex 153
6.1.8 KRN: KeyRevisionNumber 153
6.1.9 KT: KeyType 154
6.1.10 KEN: KeyExpiryNumber 154
6.1.11 DOE: DateOfExpiry 154
6.1.12 BDT: BaseDate 155
6.2 Jetons 155
6.2.1 Format de définition de jeton 155
6.2.2 Classe 0: TransferCredit 155
6.2.3 Classe 1: InitiateMeterTest/Display 156
6.2.4 Classe 2: SetMaximumPowerLimit 156
6.2.5 Classe 2: ClearCredit 157
6.2.6 Classe 2: SetTariffRate 157
6.2.7 Jeton de changement de clé défini pour le transfert de la DecoderKey de 64 bits 157
6.2.8 Jeton de changement de clé Key défini pour le transfert de la DecoderKey de 128 bits 158
6.2.9 Classe 2: ClearTamperCondition 159
6.2.10 Classe 2: SetMaximumPhasePowerUnbalanceLimit 159
6.2.11 Classe 2: SetWaterMeterFactor 160
6.2.12 Classe 2: Réservée pour l'usage selon la STS 160
6.2.13 Classe 2: Réservée pour un usage propriétaire 160

6.2.14 Classe 3: Réservée pour l'usage selon la STS 160
6.3 Éléments de données du jeton 161
6.3.1 Éléments de données utilisés dans des jetons 161
6.3.2 Classe: TokenClass 162
6.3.3 SubClass: TokenSubClass 163
6.3.4 RND: RandomNumber 163
6.3.5 TID: TokenIdentifier 164
6.3.6 Amount: TransferAmount 165
6.3.7 CRC: CyclicRedundancyCheck 169
6.3.8 Control: InitiateMeterTest/DisplayControlField 170
6.3.9 MPL: MaximumPowerLimit 171
6.3.10 MPPUL: MaximumPhasePowerUnbalanceLimit 171
6.3.11 Rate: TariffRate 171
6.3.12 WMFactor: WaterMeterFactor 171
6.3.13 Register: RegisterToClear 171
6.3.14 NKHO: NewKeyHighOrder 171
6.3.15 NKLO: NewKeyLowOrder 171
6.3.16 NKMO1: NewKeyMiddleOrder1 172
6.3.17 NKMO2: NewKeyMiddleOrder2 172
6.3.18 KENHO: KeyExpiryNumberHighOrder 172
6.3.19 KENLO: KeyExpiryNumberLowOrder 172
6.3.20 RO: RolloverKeyChange 172
6.3.21 S&E: SignAndExponent 172
6.3.22 CRC_C: CyclicRedundancyCheck_C 172
6.4 Fonctions de TCDUGeneration 173
6.4.1 Définition de la TCDU 173
6.4.2 Transposition des bits de Class (Classe) 173
6.4.3 Fonction TCDUGeneration pour les jetons de Class 0,1 et 2 174
6.4.4 Fonction de TCDUGeneration pour les jetons de changement de clé 175
6.4.5 Fonction TCDUGeneration pour le jeton Set2ndSectionDecoderKey 177
6.5 Fonctions de sécurité 177
6.5.1 Exigences générales 177
6.5.2 Attributs de clé et changements de clé 177
6.5.3 Génération de DecoderKey 186
6.5.4 STA: EncryptionAlgorithm07 194
6.5.5 DEA: EncryptionAlgorithm09 198
6.5.6 MISTY1: EncryptionAlgorithm11 198
7 Protocole de couche application de TokenCarriertoMeterInterface 201
7.1 APDU: ApplicationProtocolDataUnit 201
7.1.1 Éléments de données dans l'APDU 201
7.1.2 Token 201
7.1.3 AuthenticationResult 201
7.1.4 ValidationResult 201
7.1.5 TokenResult 202
7.2 Fonctions d'APDUExtraction 203
7.2.1 Processus d'extraction 203
7.2.2 Extraction des 2 bits de Class 205
7.2.3 Fonction APDUExtraction pour les jetons de Class 0 et Class 2 205
7.2.4 Fonction APDUExtraction pour les jetons de Class 1 206

7.2.5 Fonction APDUExtraction pour l'ensemble de jetons de changement de clé 206
7.3 Fonctions de sécurité 207
7.3.1 Attributs de clé et changements de clé 207
7.3.2 DKR: DecoderKeyRegister 208
7.3.3 STA: DecryptionAlgorithm07 209
7.3.4 DEA: DecryptionAlgorithm09 213
7.3.5 MISTY1: DecryptionAlgorithm11 213
7.3.6 TokenAuthentication 215
7.3.7 TokenValidation 216
7.3.8 TokenCancellation 217
8 Exigences du MeterApplicationProcess 217
8.1 Exigences générales 217
8.2 Acceptation / rejet de jeton 218
8.3 Indicateurs d'affichage et marquages 219
8.4 Jetons de TransferCredit 219
8.5 Jetons InitiateMeterTest/Display 219
8.6 Jetons SetMaximumPowerLimit 220
8.7 Jetons ClearCredit 220
8.8 Jetons SetTariffRate 220
8.9 Jetons de changement de clé 220
8.10 Jetons Set2ndSectionDecoderKey 221
8.11 Jetons ClearTamperCondition 221
8.12 Jetons SetMaximumPhasePowerUnbalanceLimit 221
8.13 SetWaterMeterFactor 221
8.14 Classe 2: Jetons réservés pour l'usage selon la STS 221
8.15 Classe 2: Jetons réservés pour un usage propriétaire 222
8.16 Classe 3: Jetons réservés pour l'usage selon la STS 222
9 KMS: Exigences génériques relatives au KeyManagementSystem 222
10 Maintenance des entités STS et services connexes 222
10.1 Généralités 222
10.2 Opérations 224
10.2.1 Maintenance de certification de produit 224
10.2.2 Maintenance du DSN 224
10.2.3 Maintenance du RO 224
10.2.4 Maintenance du TI 225
10.2.5 Maintenance du TID 225
10.2.6 Maintenance du SpecialReservedTokenIdentifier 225
10.2.7 Maintenance du MfrCode 225
10.2.8 Maintenance des tables de substitution 225
10.2.9 Maintenance des tables de permutation 225
10.2.10 Maintenance du SGC 225
10.2.11 Maintenance de la VendingKey 225
10.2.12 Maintenance du KRN 225
10.2.13 Maintenance du KT 226
10.2.14 Maintenance du KEN 226
10.2.15 Maintenance du CERT 226
10.2.16 Maintenance du CC 226
10.2.17 Maintenance de l'UC 226

10.2.18 Maintenance du KMCID 226
10.2.19 Maintenance du CMID 226
10.3 Normalisation 227
10.3.1 Maintenance de l'IIN 227
10.3.2 Maintenance du TCT 227
10.3.3 Maintenance du DKGA 227
10.3.4 Maintenance de l'EA 227
10.3.5 Maintenance de la TokenClass 227
10.3.6 Maintenance de la TokenSubClass 228
10.3.7 Maintenance de l'InitiateMeterTest/DisplayControlField 228
10.3.8 Maintenance de RegisterToClear 228
10.3.9 Maintenance de la BaseDate STS 228
10.3.10 Maintenance du Rate 228
10.3.11 Maintenance du WMFactor 229
10.3.12 Maintenance du MFO 229
10.3.13 Maintenance du FOIN 229
10.3.14 Maintenance des spécifications d'accompagnement 229
Annexe A (informative) Lignes directrices pour un KeyManagementSystem (KMS) 231
Annexe B (informative) Entités et identificateurs dans un système conforme à la STS 235
Annexe C (informative) Code de bonnes pratiques pour la mise en œuvre des systèmes conformes à la STS 239
C.1 Généralités 239
C.2 Services de maintenance et d'assistance fournis par la STS Association 239
C.3 Gestion de clé 239
C.3.1 Services de gestion de clé 239
C.3.2 Distribution de SupplyGroupCode et de VendingKey 239
C.3.3 Distribution de CryptographicModule 241
C.3.4 Expiration de clé 241
C.4 MeterPAN 241
C.4.1 Pratique générale 241
C.4.2 IssuerIdentificationNumbers 242
C.4.3 ManufacturerCodes 242
C.4.4 DecoderSerialNumbers 242
C.5 SpecialReservedTokenIdentifier 242
C.6 Tables de permutation et de substitution pour le STA 242
C.7 Codes EA 243
C.8 Codes de TokenCarrierType 243
C.9 Instances de MeterFunctionObject / spécifications d'accompagnement 243
C.10 TariffIndex 243
C.11 Certification de conformité à la STS 244
C.11.1 Services de certification IEC 244
C.11.2 Produits 244
C.11.3 Autorité de certification 244
C.12 Options d'approvisionnement pour les utilisateurs de systèmes conformes à la STS 244
C.13 Gestion du passage à zéro des TID 248
C.13.1 Introduction 248
C.13.2 Vue d'ensemble 249
C.13.3 Analyse d'impact 251

C.13.4 Dates de référence 252
C.13.5 Mise en œuvre 252
Bibliographie 255

Figure 1 – Organigramme fonctionnel d'un compteur à paiement générique à dispositif unique 142
Figure 2 – STS modélisée comme une pile protocolaire OSI réduite à 2 couches 143
Figure 3 – Flux de données du POSApplicationProcess vers le TokenCarrier 145
Figure 4 – Flux de données du TokenCarrier vers le MeterApplicationProcess 146
Figure 5 – Composition d'un numéro de référence de transaction 147
Figure 6 – Transposition des 2 bits de Class 173
Figure 7 – Fonction TCDUGeneration pour les jetons de Class 0, 1 et 2 174
Figure 8 – Fonction de TCDUGeneration pour les jetons de changement de clé 176
Figure 9 – Changements de DecoderKey – diagramme d'états 184
Figure 10 – DecoderKeyGenerationAlgorithm01 189
Figure 11 – DecoderKeyGenerationAlgorithm02 191
Figure 12 – STA: EncryptionAlgorithm07 194
Figure 13 – Processus de substitution de chiffrement STA 195
Figure 14 – Processus de permutation de chiffrement STA 196
Figure 15 – Processus de rotation de DecoderKey de chiffrement STA 197
Figure 16 – Exemple pratique de chiffrement STA pour un jeton de TransferCredit 198
Figure 17 – MISTY1: EncryptionAlgorithm11 199
Figure 18 – Exemple pratique de chiffrement MISTY1 pour un jeton de TransferCredit 200
Figure 19 – Fonction d'APDUExtraction 204
Figure 20 – Extraction des 2 bits de Class 205
Figure 21 – DecryptionAlgorithm07 STA 209
Figure 22 – Processus de permutation de déchiffrement STA 210
Figure 23 – Processus de substitution de déchiffrement STA 211
Figure 24 – Processus de rotation de DecoderKey de déchiffrement STA 212
Figure 25 – Exemple pratique de déchiffrement STA pour un jeton de TransferCredit 213
Figure 26 – DecryptionAlgorithm11 STA 214
Figure 27 – Exemple pratique de déchiffrement MISTY1 pour un jeton de TransferCredit 215
Figure A.1 – KeyManagementSystem et relations interactives entres des entités 231
Figure B.1 – Entités et identificateurs déployés dans un système conforme à la STS 236
Figure C.1 – Vue d'ensemble du système 250

Tableau 1 – Éléments de données dans l'APDU 148
Tableau 2 – Éléments de données dans l'IDRecord 149
Tableau 3 – Éléments de données dans le MeterPAN 149
Tableau 4 – Éléments de données dans l'IAIN / DRN 150
Tableau 5 – Types de supports de jeton 151
Tableau 6 – Codes de DKGA 152
Tableau 7 – Codes EA 152

Tableau 8 – Types de SGC et types de clés 153
Tableau 9 – Codes de DOE pour l'année 154
Tableau 10 – Codes de DOE pour le mois 155
Tableau 11 – Représentation de BDT 155
Tableau 12 – Format de définition de jeton 155
Tableau 13 – Éléments de données utilisés dans des jetons 161
Tableau 14 – Classes de jetons 162
Tableau 15 – Sous-classes de jetons 163
Tableau 16 – Exemples de calcul de TID 164
Tableau 17 – Unités de mesure pour l'électricité 165
Tableau 18 – Unités de mesure pour d'autres applications 166
Tableau 19 – Allocations des bits pour le champ Amount (montant) applicable à la SubClass 0 à 3 166
Tableau 20 – Erreur maximale d'arrondi 167
Tableau 21 – Exemples de valeurs de TransferAmount pour le transfert de crédit 167
Tableau 22 – Allocations des bits pour le champ Amount (montant) applicable à la SubClass 4 à 7 167
Tableau 23 – Allocations des bits pour l'exposant e 167
Tableau 24 – Exemples d'arrondi de valeurs négatives et positives 168
Tableau 25 – Exemples deTransferAmounts et d'erreurs d'arrondi 169
Tableau 26 – Exemple de calcul de CRC 169
Tableau 27 – Valeurs admissibles du champ Control 170
Tableau 28 – Sélection du registre à vider 171
Tableau 29 – Positions des bits S&E pour les variables s, e_4, e_3 et e_2 172
Tableau 30 – Exemple de calcul de CRC_C 172
Tableau 31 – Classification des VendingKey (clés de vente) 179
Tableau 32 – Classification des DecoderKeys (clés de décodeur) 180
Tableau 33 – Relations autorisées entre les types de clés de décodeur 185
Tableau 34 – Définition du PANBlock 187
Tableau 35 – Éléments de données dans le PANBlock 187
Tableau 36 – Définition du CONTROLBlock 187
Tableau 37 – Éléments de données dans le CONTROLBlock 188
Tableau 38 – Plage des valeurs applicables pour les numéros de référence de décodeur 188
Tableau 39 – Liste des valeurs applicables pour les codes de groupe d'alimentation 189
Tableau 40 – Éléments de données dans le DataBlock 192
Tableau 41 – Paramètres d'entrée pour un exemple pratique 193
Tableau 42 – Constitution de l'exemple de DataBlock 193
Tableau 43 – Constitution de l'exemple de DecoderKey 193
Tableau 44 – Tables de substitution d'échantillons 195
Tableau 45 – Table de permutation d'échantillons 196
Tableau 46 – Éléments de données dans l'APDU 201
Tableau 47 – Valeurs possibles de l'AuthenticationResult 201
Tableau 48 – Valeurs possibles du ValidationResult 202

Tableau 49 – Valeurs possibles du TokenResult 203
Tableau 50 – Valeurs stockées dans le DKR 208
Tableau 51 – Table de permutation d'échantillons 210
Tableau 52 – Tables de substitution d'échantillons 211
Tableau 53 – Entités/services exigeant un service de maintenance 223
Tableau A.1 – Entités qui participent aux processus de KMS 232
Tableau A.2 – Processus entourant le compteur à paiement et la DecoderKey 232
Tableau A.3 – Processus entourant le CryptographicModule (module cryptographique) 233
Tableau A.4 – Processus entourant le SGC et la VendingKey 233
Tableau B.1 – Entités types déployées dans un système conforme à la STS 236
Tableau B.2 – Identificateurs associés aux entités dans un système conforme à la STS 238
Tableau C.1 – Éléments de données associés à un SGC 240
Tableau C.2 – Éléments de données associés au CryptographicModule 241
Tableau C.3 – Éléments qu'il convient de noter dans les ordres d'achat et les soumissions d'offres 245

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62055-41 a été établie par le comité d'études 13 de l'IEC: Comptage et pilotage de l'énergie électrique.

Cette troisième édition annule et remplace la deuxième édition de l'IEC 62055-41, parue en 2014. Cette édition constitue une révision technique.

Les modifications techniques majeures par rapport à l'édition précédente sont les suivantes:

- jetons de transfert de monnaies pour le comptage de l'électricité, de l'eau, du gaz et du temps;
- résolution plus affinée du transfert de crédit pour le gaz et la durée;

- code PAN commun pour les codes de constructeur de 2 chiffres et de 4 chiffres;
- valeurs de MfrCode réservées à des fins de certification et d'essai;
- instauration d'une suite DLMS/COSEM comme type de support de jeton virtuel;
- ajout de DKGA04, fonction de dérivation de clé avancée issue de la VendingKey de 160 bits;
- suppression de DES et de TDES pour l'algorithme cryptographique EA09 et DKGA03 respectivement, mais DES pour l'algorithme DKGA02 continue à être utilisé;
- ajout de l'algorithme cryptographique MISTY1 utilisant une DecoderKey (Clé de décodeur) de 128 bits avec jetons de changement de clé de prise en charge;
- transfert des valeurs SGC au compteur par l'intermédiaire des jetons de changement de clé;
- révision des exigences concernant les jetons d'essai/affichage;
- révision du KMS afin de refléter les meilleures pratiques actuelles;
- révision des lignes directrices de gestion du passage à zéro des TID;
- définition de BaseDate référencée par rapport au Temps Universel Coordonné;
- désassociation de l'IIN de la définition de la norme ISO;
- diverses clarifications et améliorations venant à l'appui des éléments ci-dessus.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
13/1755/FDIS	13/1764/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2

Une liste de toutes les parties de la série IEC 62055, publiées sous le titre général *Comptage de l'électricité – Systèmes de paiement*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

INTRODUCTION

La série IEC 62055 couvre les systèmes de paiement, englobant les systèmes d'informations des consommateurs, les systèmes de points de vente, les supports de jetons, les compteurs de paiement et les interfaces respectives qui existent entre ces entités. Au moment de la préparation du présent document, l'IEC 62055 comprenait les parties suivantes, sous le titre général, *Comptage de l'électricité – Systèmes de paiement*:

Partie 21: Framework for standardization (disponible en anglais seulement)

Partie 31: Exigences particulières – Compteurs statiques à paiement d'énergie active (classes 1 et 2)

Partie 41: Spécification de transfert normalisé (STS) – Protocole de couche application pour les systèmes de supports de jeton unidirectionnel

Partie 42: Transfer reference numbers (TRN) – Application layer protocol for one-way token carrier systems (disponible en anglais seulement)

Partie 51: Standard transfer specification (STS) – Physical layer protocol for one-way numeric and magnetic card token carriers (disponible en anglais seulement)

Partie 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection (disponible en anglais seulement)

La série des Parties 4x spécifie les protocoles de couche application et la série des Parties 5x spécifie les protocoles de couche physique.

NOTE 1 La partie 42 n'est pas compatible avec les parties 41, 51 et 52.

NOTE 2 La partie 42 était en cours d'élaboration au moment de la publication de la présente édition de la partie 41.

La spécification de transfert normalisé (STS – *Standard transfer specification*) est un protocole de message sécurisé qui permet de transporter des informations entre des équipements de point de vente (POS – *Point of sale*) et des compteurs de paiement. Elle permet plusieurs types de messages, tels que les consignes concernant le crédit, la maîtrise de la configuration, l'affichage et les essais. Elle spécifie en outre les dispositifs et les codes de pratique qui permettent la prise en charge de la gestion sécurisée (génération, stockage, retrait et transport) des clés cryptographiques utilisées au sein du système.

Le support de jeton, qui n'est pas spécifié dans la présente partie de l'IEC 62055, est le dispositif ou support physique utilisé pour transporter les informations, et ce, de l'équipement de POS vers le compteur à paiement. Trois types de supports de jetons sont actuellement spécifiés dans l'IEC 62055-51 et l'IEC 62055-52; la carte magnétique, le support de jeton numérique et un support de jeton virtuel, qui ont été approuvés par la STS Association. De nouveaux supports de jeton peuvent être proposés comme nouveaux sujets d'étude par l'intermédiaire des Comités nationaux ou par l'intermédiaire de la STS Association.

Bien que la principale mise en œuvre de la STS se situe dans l'industrie d'alimentation en électricité, elle permet la prise en charge de la gestion d'autres services d'une entreprise de distribution comme l'eau et le gaz. Il convient de noter que certaines fonctionnalités peuvent ne pas s'appliquer dans tous les services d'une entreprise de distribution, un exemple en étant la MaximumPowerLimit (Limite de la Puissance Maximum) dans le cas d'un compteur d'eau. De même, certaines terminologies peuvent ne pas être appropriées dans des applications hors du domaine de l'électricité, un exemple en étant l'interrupteur de la charge dans le cas d'un compteur de gaz. Les révisions futures de la STS peuvent permettre la prise en charge d'autres technologies de supports de jeton comme les cartes intelligentes et les clés à mémoire avec une fonctionnalité bidirectionnelle et permettre une horloge temps réel et des tarifs complexes dans le compteur à paiement.

Toutes les exigences spécifiées dans le présent document ne sont pas obligatoires pour une mise en œuvre dans une configuration particulière de système. À titre de lignes directrices, un choix de paramètres de configuration facultatifs est énuméré à l'Article C.12.

La STS Association est enregistrée auprès de l'IEC comme une Autorité d'enregistrement destinée à fournir des services de maintenance venant à l'appui de la STS (voir l'Article C.1 pour plus d'informations).

La publication de la première édition de l'IEC 62055-41 en mai 2007 a conduit à son adoption rapide comme la norme générale préférentielle pour les compteurs de prépaiement dans de nombreux pays membres de l'IEC et dans une majorité de pays membres affiliés à l'IEC. Les compteurs d'électricité à prépaiement et leurs systèmes de paiement associés sont maintenant produits, exploités et maintenus dans un écosystème d'entreprises de distribution, de constructeurs de compteurs, d'opérateurs de compteurs, de fournisseurs de systèmes de vente, d'agents de vente, d'établissements bancaires et d'industries adjacentes. Les intérêts pluripartites sont servis par la STS Association comportant plus de 150 organisations sises dans plus de 35 pays. L'interopérabilité et la conformité à la Spécification de transfert normalisé (STS) sont garanties par des spécifications d'essai de conformité développées et gérées par la STS Association. Une liste complète des services de la STS Association peut être consultée à l'adresse http://www.sts.org.za.

Initialement développée pour des compteurs d'électricité à prépaiement en Afrique – par l'intermédiaire d'une liaison de type D du groupe de travail (GT) 15 du Comité d'études 13 de l'IEC avec la STS Association – la présente norme IEC sert maintenant plus d'utilisateurs en Asie qu'en Afrique, avec un total d'environ 50 millions de compteurs exploités par 500 entreprises de distribution dans 94 pays. La gestion de la technologie a été administrée par la STS Association dans le cadre de l'accomplissement de son rôle d'Autorité d'enregistrement désignée par l'IEC.

Face au développement constant des algorithmes cryptographiques avancés, la révision des niveaux de sécurité spécifiés dans l'IEC 62055-41 est devenue souhaitable de manière à refléter l'état de l'art des meilleures pratiques qui seront appropriées pour le déploiement de nouveaux systèmes avec une durée de vie prévisionnelle couvrant au moins les 30 prochaines années.

De même, l'évolution des systèmes de comptage intelligents avec fonctionnalité de prépaiement permet l'utilisation des fonctions de tarification dans le compteur, créant ainsi la nécessité de fournir au compteur le transfert en unités monétaires en lieu et place des unités de service.

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation d'un brevet intéressant l'identifiant du jeton spécial réservé indiqué en 6.3.5.2.

L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété.

Le détenteur de ces droits de propriété a donné l'assurance à l'IEC qu'il consent à négocier des licences avec des demandeurs du monde entier, soit sans frais, soit à des termes et conditions raisonnables et non discriminatoires. À ce propos, la déclaration du détenteur des droits de propriété est enregistrée à l'IEC. Des informations peuvent être demandées à:

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

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

L'attention est d'autre part attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété autres que ceux qui ont été mentionnés ci-dessus. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

L'ISO (www.iso.org/patents) et l'IEC (http://patents.iec.ch) tiennent à jour des bases de données, consultables en ligne, des droits de propriété liés à leurs normes. Les utilisateurs sont invités à consulter ces bases de données pour obtenir les informations les plus récentes concernant les droits de propriété.

La Commission Électrotechnique Internationale (IEC) attire l'attention sur le fait qu'il est déclaré que la conformité aux dispositions de la présente Norme internationale peut impliquer l'utilisation d'un service de maintenance concernant la gestion de clé de chiffrement et la pile de protocoles sur lesquels est basée la présente Norme internationale IEC 62055-41 [Voir Article C.1]. L'IEC ne prend pas position quant à la preuve, à la validité et la portée de ce service de maintenance.

Le fournisseur du service de maintenance a donné l'assurance à l'IEC qu'il consent à fournir ces services aux demandeurs du monde entier, à des termes et conditions raisonnables et non discriminatoires. À ce propos, la déclaration du fournisseur du service de maintenance est enregistrée à l'IEC. Des informations peuvent être demandées à

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

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

1 Domaine d'application

La présente partie de l'IEC 62055 spécifie le protocole de couche application de la STS pour transférer des unités de crédit et autres informations de gestion, et ce, d'un système de point de vente (POS) vers un compteur à paiement conforme à la STS dans un système de support de jeton unidirectionnel. Elle est destinée principalement à être appliquée avec les compteurs à paiement d'électricité simple tarif utilisant des jetons basés sur l'énergie. Elle peut également être appliquée aux systèmes de jeton basés sur la monnaie et pour les services autres que l'électricité.

Elle spécifie:

- une interface POS/support de jeton structurée avec un protocole de couche application et un protocole de couche physique utilisant le modèle OSI comme référence;
- des jetons pour le protocole de couche application pour transférer les divers messages du POS vers le compteur à paiement;
- des fonctions et des processus de sécurité dans le protocole de couche application tels que l'Algorithme de transfert normalisé (Standard Transfer Algorithm) et l'Algorithme de chiffrement de données (Data Encryption Algorithm), y compris la génération et la distribution des clés cryptographiques associées;
- des fonctions et des processus de sécurité dans le protocole de couche application au niveau du compteur à paiement tels que les algorithmes de déchiffrement, l'authentification, la validation et l'annulation de jetons;
- des exigences spécifiques relatives au processus d'application de compteur en réponse aux jetons reçus;
- une méthode pour traiter de la fonctionnalité de compteur à paiement dans le processus d'application de compteur et les spécifications d'accompagnement associées;
- des exigences génériques relatives à un système de gestion de clés conforme à la STS;
- des lignes directrices pour un système de gestion de clés;
- des entités et des identificateurs utilisés dans un système STS;
- le code de bonnes pratiques pour la gestion des changements de clé par passage à zéro de l'identificateur de jeton (TID) en association avec l'ensemble révisé de dates de référence;
- le code de bonnes pratiques et les services de support à la maintenance provenant de la STS Association.

Elle est destinée à être utilisée par les constructeurs de compteurs à paiement qui doivent accepter les jetons conformes à la STS et aussi par les constructeurs de systèmes POS qui doivent produire des jetons conformes à la STS. Elle doit être utilisée conjointement avec la série IEC 62055-5x.

Il est exigé des produits conformes à la STS de se conformer uniquement aux parties sélectives de ce document ayant été l'objet d'un contrat d'achat (voir aussi Article C.12).

NOTE Bien qu'il ait été mis au point pour les systèmes de paiement pour l'électricité, le document prévoit également des dispositions pour les jetons utilisés dans d'autres services d'entreprise de distribution, tels que l'eau et le gaz.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TR 62051:1999, *Electricity metering – Glossary of terms*(disponible en anglais seulement)

IEC TR 62055-21:2005, *Electricity metering – Payment systems – Part 21: Framework for standardization* (disponible en anglais seulement)

IEC 62055-31:2005, *Equipements de comptage de l'électricité – Systèmes à paiement – Partie 31: Exigences particulières – Compteurs statiques à paiement d'énergie active (classes 1 et 2)*

IEC 62055-51:2007, *Electricity metering – Payment systems – Part 51: Standard transfer specification (STS) – Physical layer protocol for one-way numeric and magnetic card token carriers* (disponible en anglais seulement)

IEC 62055-52:2008, *Electricity metering – Payment systems – Part 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection* (disponible en anglais seulement)

ISO/IEC 7812-1:2017, *Identification cards – Identification of issuers – Part 1: Numbering system* (disponible en anglais seulement)

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers* (disponible en anglais seulement)

ISO 9797-2, *Information technology – Security techniques – Message Authentication. Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function* (disponible en anglais seulement)

ISO 10118-3, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated Hash Functions* (disponible en anglais seulement)

ANSI X3.92-1981, *American National Standard Data Encryption Algorithm, American National Standards Institute – Data Encryption Algorithm*

FIPS PUB 46-3:1999, *Federal Information Processing Standards Publication – Data Encryption Standard*

NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*