



INTERNATIONAL STANDARD



**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 978-2-8322-1614-9

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

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	2
1 Scope.....	13
2 Normative references	13
3 Terms, definitions and abbreviations	14
3.1 Terms and definitions.....	14
3.2 Abbreviations.....	15
3.3 Notation and terminology	18
4 Numbering conventions	18
5 Reference model for the standard transfer specification	19
5.1 Generic payment meter functional reference diagram.....	19
5.2 STS protocol reference model.....	20
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier.....	21
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess.....	22
5.5 MeterFunctionObjects / companion specifications.....	23
5.6 ISO transaction reference numbers.....	23
6 POSToTokenCarrierInterface application layer protocol.....	23
6.1 APDU: ApplicationProtocolDataUnit.....	23
6.1.1 Data elements in the APDU	23
6.1.2 MeterPAN: MeterPrimaryAccountNumber	25
6.1.3 TCT: TokenCarrierType.....	26
6.1.4 DKGA: DecoderKeyGenerationAlgorithm	27
6.1.5 EA: EncryptionAlgorithm.....	27
6.1.6 SGC: SupplyGroupCode.....	28
6.1.7 TI: TariffIndex.....	28
6.1.8 KRN: KeyRevisionNumber	29
6.1.9 KT: KeyType.....	29
6.1.10 KEN: KeyExpiryNumber	29
6.1.11 DCE: DateOfExpiry.....	29
6.2 Tokens.....	30
6.2.1 Token definition format	30
6.2.2 Class 0: TransferCredit.....	30
6.2.3 Class 1: InitiateMeterTest/Display	31
6.2.4 Class 2: SetMaximumPowerLimit	31
6.2.5 Class 2: ClearCredit	31
6.2.6 Class 2: SetTariffRate	31
6.2.7 Class 2: Set1stSectionDecoderKey.....	32
6.2.8 Class 2: Set2ndSectionDecoderKey.....	32
6.2.9 Class 2: ClearTamperCondition	32
6.2.10 Class 2: SetMaximumPhasePowerUnbalanceLimit.....	32
6.2.11 Class 2: SetWaterMeterFactor.....	32
6.2.12 Class 2: Reserved for STS use.....	33
6.2.13 Class 2: Reserved for Proprietary use	33
6.2.14 Class 3: Reserved for STS use.....	33

6.3	Token data elements	33
6.3.1	Data elements used in tokens	33
6.3.2	Class: TokenClass	34
6.3.3	SubClass: TokenSubClass	34
6.3.4	RND: RandomNumber	35
6.3.5	TID: TokenIdentifier	36
6.3.6	Amount: TransferAmount	37
6.3.7	CRC: CyclicRedundancyCode	39
6.3.8	Control: InitiateMeterTest/DisplayControlField	39
6.3.9	MPL: MaximumPowerLimit	40
6.3.10	MPPUL: MaximumPhasePowerUnbalanceLimit	40
6.3.11	Rate: TariffRate	40
6.3.12	WMFactor: WaterMeterFactor	40
6.3.13	Register: RegisterToClear	40
6.3.14	NKHO: NewKeyHighOrder	40
6.3.15	NKLO: NewKeyLowOrder	40
6.3.16	KENHO: KeyExpiryNumberHighOrder	40
6.3.17	KENLO: KeyExpiryNumberLowOrder	41
6.3.18	RO: RolloverKeyChange	41
6.4	TCDUGeneration functions	41
6.4.1	Definition of the TCDU	41
6.4.2	Transposition of the Class bits	41
6.4.3	TCDUGeneration function for Class 0,1 and 2 tokens	42
6.4.4	TCDUGeneration function for Set1stSectionDecoderKey token	42
6.4.5	TCDUGeneration function for Set2ndSectionDecoderKey token	45
6.5	Security functions	46
6.5.1	General requirements	46
6.5.2	Key attributes and key changes	46
6.5.3	DecoderKey generation	54
6.5.4	STA: EncryptionAlgorithm07	59
6.5.5	DEA: EncryptionAlgorithm09	63
7	TokenCarrierToMeterInterface application layer protocol	63
7.1	APDU: ApplicationProtocolDataUnit	63
7.1.1	Data elements in the APDU	63
7.1.2	Token	64
7.1.3	AuthenticationResult	64
7.1.4	ValidationResult	64
7.1.5	TokenResult	65
7.2	APDUExtraction functions	66
7.2.1	Extraction process	66
7.2.2	Extraction of the 2 Class bits	66
7.2.3	APDUExtraction function for Class 0 and Class 2 tokens	67
7.2.4	APDUExtraction function for Class 1 tokens	68
7.2.5	APDUExtraction function for Set1stSectionDecoderKey and Set2ndSectionDecoderKey tokens	68

7.3	Security functions	69
7.3.1	Key attributes and key changes	69
7.3.2	DKR: DecoderKeyRegister.....	69
7.3.3	STA: DecryptionAlgorithm07.....	70
7.3.4	DEA: DecryptionAlgorithm09	72
7.3.5	TokenAuthentication	73
7.3.6	TokenValidation.....	74
7.3.7	TokenCancellation	74
8	MeterApplicationProcess requirements	75
8.1	General requirements	75
8.2	Token acceptance/rejection	75
8.3	Display indicators and markings.....	76
8.4	TransferCredit tokens	77
8.5	InitiateMeterTest/Display tokens	77
8.6	SetMaximumPowerLimit tokens.....	77
8.7	ClearCredit tokens	78
8.8	SetTariffRate tokens	78
8.9	Set1stSectionDecoderKey tokens	78
8.10	Set2ndSectionDecoderKey tokens	78
8.11	ClearTamperCondition tokens.....	78
8.12	SetMaximumPhasePowerUnbalanceLimit tokens	79
8.13	SetWaterMeterFactor.....	79
8.14	Class 2: Reserved for STS use tokens	79
8.15	Class 2: Reserved for Proprietary use tokens	79
8.16	Class 3: Reserved for STS use tokens	79
9	KMS: KeyManagementSystem generic requirements	79
10	Maintenance of STS entities and related services	80
10.1	General.....	80
10.2	Operations	82
10.2.1	Product certification maintenance	82
10.2.2	DSN maintenance	82
10.2.3	RO maintenance.....	82
10.2.4	TI maintenance.....	82
10.2.5	TID maintenance	83
10.2.6	SpecialReservedTokenIdentifier maintenance.....	83
10.2.7	MfrCode maintenance.....	83
10.2.8	Substitution tables maintenance	83
10.2.9	Permutation tables maintenance.....	83
10.2.10	SGC maintenance	83
10.2.11	VendingKey maintenance	83
10.2.12	KRN maintenance.....	83
10.2.13	KT maintenance	83
10.2.14	KEN maintenance.....	84
10.2.15	KEK maintenance	84
10.2.16	CC maintenance	84
10.2.17	UC maintenance	84
10.2.18	KMCID maintenance.....	84
10.2.19	CMID maintenance	84
10.2.20	CMAC maintenance.....	84

10.3	Standardisation.....	85
10.3.1	IIN maintenance	85
10.3.2	TCT maintenance	85
10.3.3	DKGA maintenance	85
10.3.4	EA maintenance	85
10.3.5	TokenClass maintenance.....	85
10.3.6	TokenSubClass maintenance.....	85
10.3.7	InitiateMeterTest/DisplayControlField maintenance.....	86
10.3.8	RegisterToClear maintenance.....	86
10.3.9	STS base date maintenance	86
10.3.10	Rate maintenance.....	86
10.3.11	WMFactor maintenance	86
10.3.12	MFO maintenance	87
10.3.13	FOIN maintenance.....	87
10.3.14	Companion specification maintenance	87
Annex A (informative)	Guidelines for a KeyManagementSystem (KMS).....	88
Annex B (informative)	Entities and identifiers in an STS-compliant system.....	91
Annex C (informative)	Code of practice for the implementation of STS-compliant systems.....	95
C.1	Maintenance and support services provided by the STS Association.....	95
C.2	Key management.....	95
C.2.1	Key management services.....	95
C.2.2	SupplyGroupCode and VendingKey distribution	95
C.2.3	CryptographicModule distribution.....	96
C.2.4	Key expiry	97
C.3	MeterPAN	97
C.3.1	General practice	97
C.3.2	IssuerIdentificationNumbers	97
C.3.3	ManufacturerCodes	97
C.3.4	DecoderSerialNumbers.....	98
C.4	SpecialReservedTokenIdentifier.....	98
C.5	Permutation and substitution tables for the STA.....	99
C.6	EA codes	99
C.7	TokenCarrierType codes.....	99
C.8	MeterFunctionObject instances / companion specifications	99
C.9	TariffIndex	99
C.10	STS-compliance certification.....	100
C.10.1	IEC certification services	100
C.10.2	Products	100
C.10.3	Certification authority.....	100
C.11	Procurement options for users of STS-compliant systems.....	100
C.12	Management of TID Rollover.....	104
C.12.1	Introduction	104
C.12.2	Overview	105
C.12.3	Impact analysis.....	107
C.12.4	Base dates	108
C.12.5	Implementation	108
Bibliography	110

Figure 1 – Functional block diagram of a generic single-part payment meter.....	19
Figure 2 – STS modelled as a 2-layer collapsed OSI protocol stack.....	20
Figure 3 – Dataflow from the POSApplicationProcess to the TokenCarrier.....	21
Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess.....	22
Figure 5 – Composition of ISO transaction reference number.....	23
Figure 6 – Transposition of the 2 Class bits.....	41
Figure 7 – TCDUGeneration function for Class 0, 1 and 2 tokens.....	42
Figure 8 – TCDUGeneration function for Set1stSectionDecoderKey token.....	43
Figure 9 – TCDUGeneration function for Set2ndSectionDecoderKey token.....	45
Figure 10 – DecoderKey changes – state diagram.....	51
Figure 11 – DecoderKeyGenerationAlgorithm01.....	56
Figure 12 – DecoderKeyGenerationAlgorithm02.....	57
Figure 13 – DecoderKeyGenerationAlgorithm03.....	58
Figure 14 – STA: EncryptionAlgorithm07.....	59
Figure 15 – STA encryption substitution process.....	60
Figure 16 – STA encryption permutation process.....	61
Figure 17 – STA encryption DecoderKey rotation process.....	61
Figure 18 – STA encryption worked example for TransferCredit token.....	62
Figure 19 – DEA: EncryptionAlgorithm09.....	63
Figure 20 – APDUExtraction function.....	66
Figure 21 – Extraction of the 2 Class bits.....	67
Figure 22 – STA DecryptionAlgorithm07.....	70
Figure 23 – STA decryption permutation process.....	70
Figure 24 – STA decryption substitution process.....	71
Figure 25 – STA decryption DecoderKey rotation process.....	72
Figure 26 – STA decryption worked example for TransferCredit token.....	72
Figure 27 – DEA DecryptionAlgorithm09.....	73
Figure A.1 – KeyManagementSystem and interactive relationships between entities.....	88
Figure B.1 – Entities and identifiers deployed in an STS-compliant system.....	91
Figure C.1 – System overview.....	106
Table 1 – Data elements in the APDU.....	24
Table 2 – Data elements in the IDRecord.....	24
Table 3 – Data elements in the MeterPAN.....	25
Table 4 – Data elements in the IAIN / DRN.....	26
Table 5 – Token carrier types.....	27
Table 6 – DKGA codes.....	27
Table 7 – EA codes.....	28
Table 8 – SGC types and key types.....	28
Table 9 – DOE codes for the year.....	30
Table 10 – DOE codes for the month.....	30
Table 11 –Token definition format.....	30
Table 12 – Data elements used in tokens.....	33

Table 13 – Token classes	34
Table 14 – Token sub-classes	35
Table 15 – TID calculation examples	36
Table 16 – Units of measure for electricity	37
Table 17 – Units of measure for other applications	37
Table 18 – Bit allocations for the TransferAmount	38
Table 19 – Maximum error due to rounding	38
Table 20 – Examples of TransferAmount values for credit transfer	38
Table 21 – Example of a CRC calculation	39
Table 22 – Permissible control field values	39
Table 23 – Selection of register to clear	40
Table 24 – Classification of vending keys	47
Table 25 – Classification of decoder keys	48
Table 26 – Permitted relationships between decoder key types	52
Table 27 – Definition of the PANBlock	54
Table 28 – Data elements in the PANBlock	54
Table 29 – Definition of the CONTROLBlock	55
Table 30 – Data elements in the CONTROLBlock	55
Table 31 – Range of applicable decoder reference numbers	55
Table 32 – List of applicable supply group codes	56
Table 33 – Sample substitution tables	60
Table 34 – Sample permutation table	61
Table 35 – Data elements in the APDU	64
Table 36 – Possible values for the AuthenticationResult	64
Table 37 – Possible values for the ValidationResult	65
Table 38 – Possible values for the TokenResult	65
Table 39 – Values stored in the DKP	69
Table 40 – Sample permutation table	70
Table 41 – Sample substitution tables	71
Table 42 – Entities/services requiring maintenance service	81
Table A.1 – Entities that participate in KMS processes	88
Table A.2 – Processes surrounding the payment meter and DecoderKey	89
Table A.3 – Processes surrounding the CryptographicModule	89
Table A.4 – Processes surrounding the SGC and VendingKey	90
Table B.1 – Typical entities deployed in an STS-compliant system	92
Table B.2 – Identifiers associated with the entities in an STS-compliant system	93
Table C.1 – Data elements associated with a SGC	96
Table C.2 – Data elements associated with the CryptographicModule	97
Table C.3 – Items that should be noted in purchase orders and tenders	100

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.

This redline version of the official IEC Standard allows the user to identify the changes made to the 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 second edition cancels and replaces the first edition issued in 2007. It constitutes a technical revision. The main technical changes with regard to the previous edition are as follows:

- Class 2 token is extended to include credit transfer for gas and water with associated extensions in the display/test tokens.
- MfrCode is extended from 2 to 4 digits.
- Three token identifier base dates are defined to provide for more frequent key changes with TID roll-over procedures.
- A code of practice for the management of TID roll-over key changes in association with the revised set of base dates.
- Some clarifications and additional examples have been added.

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

CDV	Report on voting
13/1530/CDV	13/1553/RVC

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

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.

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

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

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

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 standard, 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 – Application layer protocol for one-way token carrier systems

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

Part 52: Standard transfer specification – 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.

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 national electricity utility in South Africa (Eskom) first developed and published the STS in 1993 and transferred ownership to the STS Association in 1998 for management and further development. It is currently the only open system for one-way payment meters and to date there are more than 4 million STS payment meters in the field, being used by approximately 400 utilities in 28 countries. The STS has been stable for 10 years, is the *de facto* industry standard at national and international level and hence has been developed as an IEC standard with the appropriate reformatting to comply with WG15 work. The primary application of the STS has been for use with payment meters without a tariff employing energy-based tokens, but it could be applied to currency-based token systems.~~

~~Prior to the development of the STS a variety of proprietary payment meters and POS equipment had been developed, which were, however, not compatible with each other. This gave rise to a definite need among the major users to move towards standardized solutions in addressing operational problems experienced where various types of payment meter and POS equipment had to be operated simultaneously. A standard transfer specification was developed that would allow for the application and inter-operability of payment meters and POS equipment from multiple manufacturers in a payment metering installation.~~

~~Two encryption algorithms are in this standard. The STA is used in existing systems, while the DEA may be considered for future systems.~~

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 standard are compulsory for implementation in a particular system configuration and as a guideline, a selection of optional configuration parameters are listed in Clause C.11.

~~The STS Association has established D-type liaison with working group 15 of IEC TC 13 for the development of standards within the scope of the STS and is thus responsible for the maintenance of any such IEC standards that might be developed as a result of this liaison.~~

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 IEC 62055-41 Ed 1 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 organisations located in over 24 countries. Interoperability and conformance to the Standard Transfer System (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 million meters operated by 400 utilities in 30 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 IEC CB scheme

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: sts@vdw.co.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 data;
- 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 International Standard only, which is the subject of the purchase contract (see also Clause C.11).

NOTE 1 Although developed for payment systems for electricity, the standard also makes provision for tokens used in other utility services, such as water and gas.

~~NOTE 2 STS-compliant products are required to comply with selective parts of this International Standard only, which should be the subject of the purchase contract (see also C.11).~~

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 60050-300, *International Electrotechnical Vocabulary (IEV) – Electrical and electronic measurements and measuring instruments – Part 311: General terms relating to measurements – Part 312: General terms relating to electrical measurements – Part 313: Types of electrical measuring instruments – Part 314: Specific terms according to the type of instrument*~~

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

IEC 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, *Identification cards – Identification of issuers – Part 1: Numbering system*

ISO/IEC 7812-2:2000/2007, *Identification cards – Identification of issuers – Part 2: Application and registration procedures*

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*

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**

WILSON

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	13
2 Normative references	13
3 Terms, definitions and abbreviations	14
3.1 Terms and definitions.....	14
3.2 Abbreviations.....	15
3.3 Notation and terminology	17
4 Numbering conventions	18
5 Reference model for the standard transfer specification	19
5.1 Generic payment meter functional reference diagram	19
5.2 STS protocol reference model.....	20
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier.....	21
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess	22
5.5 MeterFunctionObjects / companion specifications	23
5.6 ISO transaction reference numbers.....	23
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	25
6.1.3 TCT: TokenCarrierType	27
6.1.4 DKGA: DecoderKeyGenerationAlgorithm	27
6.1.5 EA: EncryptionAlgorithm.....	27
6.1.6 SGC: SupplyGroupCode.....	28
6.1.7 TI: TariffIndex	28
6.1.8 KRN: KeyRevisionNumber	29
6.1.9 KT: KeyType.....	29
6.1.10 KEN: KeyExpiryNumber	29
6.1.11 DOE: DateOfExpiry.....	29
6.2 Tokens.....	30
6.2.1 Token definition format	30
6.2.2 Class 0: TransferCredit.....	30
6.2.3 Class 1: InitiateMeterTest/Display	31
6.2.4 Class 2: SetMaximumPowerLimit	31
6.2.5 Class 2: ClearCredit	31
6.2.6 Class 2: SetTariffRate	31
6.2.7 Class 2: Set1stSectionDecoderKey.....	32
6.2.8 Class 2: Set2ndSectionDecoderKey.....	32
6.2.9 Class 2: ClearTamperCondition	32
6.2.10 Class 2: SetMaximumPhasePowerUnbalanceLimit.....	33
6.2.11 Class 2: SetWaterMeterFactor	33
6.2.12 Class 2: Reserved for STS use.....	33
6.2.13 Class 2: Reserved for Proprietary use	33
6.2.14 Class 3: Reserved for STS use.....	33

6.3	Token data elements	34
6.3.1	Data elements used in tokens	34
6.3.2	Class: TokenClass	35
6.3.3	SubClass: TokenSubClass	35
6.3.4	RND: RandomNumber	36
6.3.5	TID: TokenIdentifier	36
6.3.6	Amount: TransferAmount	38
6.3.7	CRC: CyclicRedundancyCode	39
6.3.8	Control: InitiateMeterTest/DisplayControlField	40
6.3.9	MPL: MaximumPowerLimit	41
6.3.10	MPPUL: MaximumPhasePowerUnbalanceLimit	41
6.3.11	Rate: TariffRate	41
6.3.12	WMFactor: WaterMeterFactor	41
6.3.13	Register: RegisterToClear	41
6.3.14	NKHO: NewKeyHighOrder	41
6.3.15	NKLO: NewKeyLowOrder	41
6.3.16	KENHO: KeyExpiryNumberHighOrder	41
6.3.17	KENLO: KeyExpiryNumberLowOrder	41
6.3.18	RO: RolloverKeyChange	42
6.4	TCDUGeneration functions	42
6.4.1	Definition of the TCDU	42
6.4.2	Transposition of the Class bits	42
6.4.3	TCDUGeneration function for Class 0,1 and 2 tokens	43
6.4.4	TCDUGeneration function for Set1stSectionDecoderKey token	44
6.4.5	TCDUGeneration function for Set2ndSectionDecoderKey token	46
6.5	Security functions	47
6.5.1	General requirements	47
6.5.2	Key attributes and key changes	47
6.5.3	DecoderKey generation	55
6.5.4	STA: EncryptionAlgorithm07	60
6.5.5	DEA: EncryptionAlgorithm09	64
7	TokenCarrierToMeterInterface application layer protocol	64
7.1	APDU: ApplicationProtocolDataUnit	64
7.1.1	Data elements in the APDU	64
7.1.2	Token	65
7.1.3	AuthenticationResult	65
7.1.4	ValidationResult	65
7.1.5	TokenResult	66
7.2	APDUExtraction functions	67
7.2.1	Extraction process	67
7.2.2	Extraction of the 2 Class bits	67
7.2.3	APDUExtraction function for Class 0 and Class 2 tokens	68
7.2.4	APDUExtraction function for Class 1 tokens	69
7.2.5	APDUExtraction function for Set1stSectionDecoderKey and Set2ndSectionDecoderKey tokens	69
7.3	Security functions	70
7.3.1	Key attributes and key changes	70
7.3.2	DKR: DecoderKeyRegister	70
7.3.3	STA: DecryptionAlgorithm07	71

7.3.4	DEA: DecryptionAlgorithm09	74
7.3.5	TokenAuthentication	74
7.3.6	TokenValidation	75
7.3.7	TokenCancellation	75
8	MeterApplicationProcess requirements	76
8.1	General requirements	76
8.2	Token acceptance/rejection	76
8.3	Display indicators and markings	77
8.4	TransferCredit tokens	78
8.5	InitiateMeterTest/Display tokens	78
8.6	SetMaximumPowerLimit tokens	78
8.7	ClearCredit tokens	79
8.8	SetTariffRate tokens	79
8.9	Set1stSectionDecoderKey tokens	79
8.10	Set2ndSectionDecoderKey tokens	79
8.11	ClearTamperCondition tokens	79
8.12	SetMaximumPhasePowerUnbalanceLimit tokens	80
8.13	SetWaterMeterFactor	80
8.14	Class 2: Reserved for STS use tokens	80
8.15	Class 2: Reserved for Proprietary use tokens	80
8.16	Class 3: Reserved for STS use tokens	80
9	KMS: KeyManagementSystem generic requirements	80
10	Maintenance of STS entities and related services	81
10.1	General	81
10.2	Operations	83
10.2.1	Product certification maintenance	83
10.2.2	DSN maintenance	83
10.2.3	RO maintenance	83
10.2.4	TI maintenance	84
10.2.5	TID maintenance	84
10.2.6	SpecialReservedTokenIdentifier maintenance	84
10.2.7	MfrCode maintenance	84
10.2.8	Substitution tables maintenance	84
10.2.9	Permutation tables maintenance	84
10.2.10	SGC maintenance	84
10.2.11	VendingKey maintenance	84
10.2.12	KRN maintenance	84
10.2.13	KT maintenance	84
10.2.14	KEN maintenance	85
10.2.15	KEK maintenance	85
10.2.16	CC maintenance	85
10.2.17	UC maintenance	85
10.2.18	KMCID maintenance	85
10.2.19	CMID maintenance	85
10.2.20	CMAC maintenance	85
10.3	Standardisation	86
10.3.1	IIN maintenance	86
10.3.2	TCT maintenance	86
10.3.3	DKGA maintenance	86

10.3.4	EA maintenance	86
10.3.5	TokenClass maintenance.....	86
10.3.6	TokenSubClass maintenance.....	87
10.3.7	InitiateMeterTest/DisplayControlField maintenance.....	87
10.3.8	RegisterToClear maintenance.....	87
10.3.9	STS base date maintenance	87
10.3.10	Rate maintenance.....	87
10.3.11	WMFactor maintenance	87
10.3.12	MFO maintenance	88
10.3.13	FOIN maintenance.....	88
10.3.14	Companion specification maintenance.....	88
Annex A (informative)	Guidelines for a KeyManagementSystem (KMS).....	89
Annex B (informative)	Entities and identifiers in an STS-compliant system.....	92
Annex C (informative)	Code of practice for the implementation of STS-compliant systems.....	96
C.1	Maintenance and support services provided by the STS Association.....	96
C.2	Key management.....	96
C.2.1	Key management services	96
C.2.2	SupplyGroupCode and VendingKey distribution.....	96
C.2.3	CryptographicModule distribution.....	97
C.2.4	Key expiry	98
C.3	MeterPAN	98
C.3.1	General practice	98
C.3.2	IssuerIdentificationNumbers	98
C.3.3	ManufacturerCodes	98
C.3.4	DecoderSerialNumbers.....	99
C.4	SpecialReservedTokenIdentifier.....	99
C.5	Permutation and substitution tables for the STA.....	99
C.6	EA codes	99
C.7	TokenCarrierType codes.....	99
C.8	MeterFunctionObject instances / companion specifications	100
C.9	TariffIndex.....	100
C.10	STS-compliance certification.....	100
C.10.1	IEC certification services	100
C.10.2	Products.....	100
C.10.3	Certification authority.....	100
C.11	Procurement options for users of STS-compliant systems.....	100
C.12	Management of TID Rollover.....	104
C.12.1	Introduction	104
C.12.2	Overview	105
C.12.3	Impact analysis.....	107
C.12.4	Base dates	107
C.12.5	Implementation.....	107
Bibliography.....		110
Figure 1 –	Functional block diagram of a generic single-part payment meter.....	19
Figure 2 –	STS modelled as a 2-layer collapsed OSI protocol stack.....	20
Figure 3 –	Dataflow from the POSApplicationProcess to the TokenCarrier.....	21

Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess	22
Figure 5 – Composition of ISO transaction reference number	23
Figure 6 – Transposition of the 2 Class bits	42
Figure 7 – TCDUGeneration function for Class 0, 1 and 2 tokens	43
Figure 8 – TCDUGeneration function for Set1stSectionDecoderKey token	44
Figure 9 – TCDUGeneration function for Set2ndSectionDecoderKey token	46
Figure 10 – DecoderKey changes – state diagram	52
Figure 11 – DecoderKeyGenerationAlgorithm01	57
Figure 12 – DecoderKeyGenerationAlgorithm02	58
Figure 13 – DecoderKeyGenerationAlgorithm03	59
Figure 14 – STA: EncryptionAlgorithm07	60
Figure 15 – STA encryption substitution process	61
Figure 16 – STA encryption permutation process	62
Figure 17 – STA encryption DecoderKey rotation process	62
Figure 18 – STA encryption worked example for TransferCredit token	63
Figure 19 – DEA: EncryptionAlgorithm09	64
Figure 20 – APDUExtraction function	67
Figure 21 – Extraction of the 2 Class bits	68
Figure 22 – STA DecryptionAlgorithm07	71
Figure 23 – STA decryption permutation process	71
Figure 24 – STA decryption substitution process	72
Figure 25 – STA decryption DecoderKey rotation process	73
Figure 26 – STA decryption worked example for TransferCredit token	73
Figure 27 – DEA DecryptionAlgorithm09	74
Figure A.1 – KeyManagementSystem and interactive relationships between entities	89
Figure B.1 – Entities and identifiers deployed in an STS-compliant system	92
Figure C.1 – System overview	105
Table 1 – Data elements in the APDU	24
Table 2 – Data elements in the IDRecord	25
Table 3 – Data elements in the MeterPAN	25
Table 4 – Data elements in the IAIN / DRN	26
Table 5 – Token carrier types	27
Table 6 – DKGA codes	27
Table 7 – EA codes	28
Table 8 – SGC types and key types	28
Table 9 – DOE codes for the year	30
Table 10 – DOE codes for the month	30
Table 11 –Token definition format	30
Table 12 – Data elements used in tokens	34
Table 13 – Token classes	35
Table 14 – Token sub-classes	36
Table 15 – TID calculation examples	37

Table 16 – Units of measure for electricity	38
Table 17 – Units of measure for other applications	38
Table 18 – Bit allocations for the TransferAmount	39
Table 19 – Maximum error due to rounding	39
Table 20 – Examples of TransferAmount values for credit transfer	39
Table 21 – Example of a CRC calculation	40
Table 22 – Permissible control field values	40
Table 23 – Selection of register to clear	41
Table 24 – Classification of vending keys	48
Table 25 – Classification of decoder keys	49
Table 26 – Permitted relationships between decoder key types	53
Table 27 – Definition of the PANBlock	55
Table 28 – Data elements in the PANBlock	55
Table 29 – Definition of the CONTROLBlock	55
Table 30 – Data elements in the CONTROLBlock	56
Table 31 – Range of applicable decoder reference numbers	56
Table 32 – List of applicable supply group codes	57
Table 33 – Sample substitution tables	61
Table 34 – Sample permutation table	62
Table 35 – Data elements in the APDU	65
Table 36 – Possible values for the AuthenticationResult	65
Table 37 – Possible values for the ValidationResult	66
Table 38 – Possible values for the TokenResult	66
Table 39 – Values stored in the DKR	70
Table 40 – Sample permutation table	71
Table 41 – Sample substitution tables	72
Table 42 – Entities/services requiring maintenance service	82
Table A.1 – Entities that participate in KMS processes	89
Table A.2 – Processes surrounding the payment meter and DecoderKey	90
Table A.3 – Processes surrounding the CryptographicModule	90
Table A.4 – Processes surrounding the SGC and VendingKey	91
Table B.1 – Typical entities deployed in an STS-compliant system	93
Table B.2 – Identifiers associated with the entities in an STS-compliant system	94
Table C.1 – Data elements associated with a SGC	97
Table C.2 – Data elements associated with the CryptographicModule	98
Table C.3 – Items that should be noted in purchase orders and tenders	101

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.

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

This second edition cancels and replaces the first edition issued in 2007. It constitutes a technical revision. The main technical changes with regard to the previous edition are as follows:

- Class 2 token is extended to include credit transfer for gas and water with associated extensions in the display/test tokens.
- MfrCode is extended from 2 to 4 digits.
- Three token identifier base dates are defined to provide for more frequent key changes with TID roll-over procedures.
- A code of practice for the management of TID roll-over key changes in association with the revised set of base dates.
- Some clarifications and additional examples have been added.

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

CDV	Report on voting
13/1530/CDV	13/1553/RVC

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

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.

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

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

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

Withdrawn

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 standard, 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 – Application layer protocol for one-way token carrier systems

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

Part 52: Standard transfer specification – 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.

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 standard are compulsory for implementation in a particular system configuration and as a guideline, a selection of optional configuration parameters are listed in Clause C.11.

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 IEC 62055-41 Ed 1 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 organisations located in over 24 countries. Interoperability and conformance to the Standard Transfer System (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 million meters operated by 400 utilities in 30 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 IEC CB scheme

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: sts@vdw.co.za

Website: <http://www.sts.org.za>

Withdrawing

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 International Standard only, which is the subject of the purchase contract (see also Clause C.11).

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 62051:1999, *Electricity metering – Glossary of terms*

IEC 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, *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*

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*

WITNESS

SOMMAIRE

AVANT-PROPOS.....	118
INTRODUCTION.....	120
1 Domaine d'application	123
2 Références normatives	124
3 Termes, définitions et abréviations	124
3.1 Termes et définitions	124
3.2 Abréviations.....	126
3.3 Notation et terminologie	128
4 Conventions de numérotation	128
5 Modèle de référence pour la spécification de transfert normalisé.....	129
5.1 Diagramme fonctionnel de référence pour compteur à paiement générique.....	129
5.2 Modèle de référence de protocole STS	131
5.3 Flux de données du POSApplicationProcess vers le TokenCarrier.....	132
5.4 Flux de données du TokenCarrier vers le MeterApplicationProcess	134
5.5 MeterFunctionObjects / spécifications d'accompagnement.....	135
5.6 Numéros de référence des transactions ISO	136
6 Protocole de couche application POSToTokenCarrierInterface	137
6.1 APDU: ApplicationProtocolDataUnit.....	137
6.1.1 Éléments de données dans l'APDU.....	137
6.1.2 MeterPAN: MeterPrimaryAccountNumber	138
6.1.3 TCT: TokenCarrierType	140
6.1.4 DKGA: DecoderKeyGenerationAlgorithm	140
6.1.5 EA: EncryptionAlgorithm.....	141
6.1.6 SGC: SupplyGroupCode.....	141
6.1.7 TI: TariffIndex	142
6.1.8 KRN: KeyRevisionNumber	142
6.1.9 KT: KeyType.....	142
6.1.10 KEN: KeyExpiryNumber	142
6.1.11 DOE: DateOfExpiry.....	142
6.2 Jetons.....	143
6.2.1 Format de définition de jeton	143
6.2.2 Classe 0: TransferCredit.....	144
6.2.3 Classe 1: InitiateMeterTest/Display.....	144
6.2.4 Classe 2: SetMaximumPowerLimit	144
6.2.5 Classe 2: ClearCredit	145
6.2.6 Classe 2: SetTariffRate.....	145
6.2.7 Classe 2: Set1stSectionDecoderKey.....	145
6.2.8 Classe 2: Set2ndSectionDecoderKey.....	145
6.2.9 Classe 2: ClearTamperCondition	145
6.2.10 Classe 2: SetMaximumPhasePowerUnbalanceLimit.....	146
6.2.11 Classe 2: SetWaterMeterFactor	146
6.2.12 Classe 2: Réservée pour l'usage selon la STS.....	146
6.2.13 Classe 2: Réservée pour un usage propriétaire	146
6.2.14 Classe 3: Réservée pour l'usage selon la STS.....	147

6.3	Éléments de données du jeton	147
6.3.1	Éléments de données utilisés dans des jetons	147
6.3.2	Classe: TokenClass	148
6.3.3	SubClass: TokenSubClass.....	148
6.3.4	RND: RandomNumber	149
6.3.5	TID: TokenIdentifier	150
6.3.6	Amount: TransferAmount	151
6.3.7	CRC: CyclicRedundancyCode	153
6.3.8	Control: InitiateMeterTest/DisplayControlField	153
6.3.9	MPL: MaximumPowerLimit.....	154
6.3.10	MPPUL: MaximumPhasePowerUnbalanceLimit	154
6.3.11	Rate: TariffRate	155
6.3.12	WMFactor: WaterMeterFactor	155
6.3.13	Register: RegisterToClear	155
6.3.14	NKHO: NewKeyHighOrder	155
6.3.15	NKLO: NewKeyLowOrder.....	155
6.3.16	KENHO: KeyExpiryNumberHighOrder	155
6.3.17	KENLO: KeyExpiryNumberLowOrder	155
6.3.18	RO: RolloverKeyChange.....	155
6.4	Fonctions de TCDUGeneration	156
6.4.1	Définition de la TCDU	156
6.4.2	Transposition des bits de Class (Classe).....	156
6.4.3	Fonction TCDUGeneration pour les jetons de Class 0,1 et 2.....	157
6.4.4	Fonction TCDUGeneration pour le jeton Set1stSectionDecoderKey	159
6.4.5	Fonction TCDUGeneration pour le jeton Set2ndSectionDecoderKey	161
6.5	Fonctions de sécurité.....	163
6.5.1	Exigences générales	163
6.5.2	Attributs de clé et changements de clé	163
6.5.3	Génération de DecoderKey.....	172
6.5.4	STA: EncryptionAlgorithm07	177
6.5.5	DEA: EncryptionAlgorithm09.....	183
7	Protocole de couche application de TokenCarriertoMeterInterface.....	184
7.1	APDU: ApplicationProtocolDataUnit	184
7.1.1	Éléments de données dans l'APDU	184
7.1.2	Token	184
7.1.3	AuthenticationResult.....	184
7.1.4	ValidationResult	184
7.1.5	TokenResult	185
7.2	Fonctions d'APDUExtraction	186
7.2.1	Processus d'extraction.....	186
7.2.2	Extraction des 2 bits de Class.....	187
7.2.3	Fonction APDUExtraction pour les jetons de Class 0 et Class 2.....	188
7.2.4	Fonction APDUExtraction pour les jetons de Class 1	188
7.2.5	Fonction APDUExtraction pour les jetons Set1stSectionDecoderKey et Set2ndSectionDecoderKey	188
7.3	Fonctions de sécurité.....	189
7.3.1	Attributs de clé et changements de clé	189
7.3.2	DKR: DecoderKeyRegister.....	190
7.3.3	STA: DecryptionAlgorithm07	191

7.3.4	DEA: DecryptionAlgorithm09.....	196
7.3.5	TokenAuthentication.....	197
7.3.6	TokenValidation.....	197
7.3.7	TokenCancellation.....	198
8	Exigences du MeterApplicationProcess.....	199
8.1	Exigences générales.....	199
8.2	Acceptation / rejet de jeton.....	199
8.3	Indicateurs d'affichage et marquages.....	200
8.4	Jetons de TransferCredit.....	200
8.5	Jetons InitiateMeterTest/Display.....	201
8.6	Jetons SetMaximumPowerLimit.....	201
8.7	Jetons ClearCredit.....	201
8.8	Jetons SetTariffRate.....	202
8.9	Jetons Set1stSectionDecoderKey.....	202
8.10	Jetons Set2ndSectionDecoderKey.....	202
8.11	Jetons ClearTamperCondition.....	202
8.12	Jetons SetMaximumPhasePowerUnbalanceLimit.....	202
8.13	SetWaterMeterFactor.....	203
8.14	Classe 2: Jetons réservés pour l'usage selon la STS.....	203
8.15	Classe 2: Jetons réservés pour un usage propriétaire.....	203
8.16	Classe 3: Jetons réservés pour l'usage selon la STS.....	203
9	KMS: Exigences génériques relatives au KeyManagementSystem.....	203
10	Maintenance des entités STS et services connexes.....	204
10.1	Généralités.....	204
10.2	Opérations.....	206
10.2.1	Maintenance de certification de produit.....	206
10.2.2	Maintenance du DSN.....	206
10.2.3	Maintenance du RO.....	206
10.2.4	Maintenance du TI.....	206
10.2.5	Maintenance du TID.....	207
10.2.6	Maintenance du SpecialReservedTokenIdentifier.....	207
10.2.7	Maintenance du MfrCode.....	207
10.2.8	Maintenance des tables de substitution.....	207
10.2.9	Maintenance des tables de permutation.....	207
10.2.10	Maintenance du SGC.....	207
10.2.11	Maintenance de la VendingKey.....	207
10.2.12	Maintenance du KRN.....	207
10.2.13	Maintenance du KT.....	207
10.2.14	Maintenance du KEN.....	208
10.2.15	Maintenance de la KEK.....	208
10.2.16	Maintenance du CC.....	208
10.2.17	Maintenance de l'UC.....	208
10.2.18	Maintenance du KMCID.....	208
10.2.19	Maintenance du CMID.....	208
10.2.20	Maintenance du CMAC.....	209
10.3	Normalisation.....	209
10.3.1	Maintenance de l'IIN.....	209
10.3.2	Maintenance du TCT.....	209
10.3.3	Maintenance du DKGA.....	209

10.3.4	Maintenance de l'EA	209
10.3.5	Maintenance de la TokenClass	210
10.3.6	Maintenance de la TokenSubClass	210
10.3.7	Maintenance de l'InitiateMeterTest/DisplayControlField	210
10.3.8	Maintenance de RegisterToClear	210
10.3.9	Maintenance de la date de référence STS (STS base date)	210
10.3.10	Maintenance du Rate	211
10.3.11	Maintenance du WMFactor	211
10.3.12	Maintenance du MFO	211
10.3.13	Maintenance du FOIN	211
10.3.14	Maintenance de la Spécification d'accompagnement	212
Annexe A (informative)	Lignes directrices pour un KeyManagementSystem (KMS)	213
Annexe B (informative)	Entités et identificateurs dans un système conforme à la STS	217
Annexe C (informative)	Code de bonnes pratiques pour la mise en œuvre des systèmes conformes à la STS	222
C.1	Services de maintenance et d'assistance fournis par la STS Association	222
C.2	Gestion de clé	222
C.2.1	Services de gestion de clé	222
C.2.2	Distribution de SupplyGroupCode et de VendingKey	222
C.2.3	Distribution de CryptographicModule	224
C.2.4	Expiration de clé	224
C.3	MeterPAN	224
C.3.1	Pratique générale	224
C.3.2	IssuerIdentificationNumbers	225
C.3.3	ManufacturerCodes	225
C.3.4	DecoderSerialNumbers	225
C.4	SpecialReservedTokenIdentifier	225
C.5	Tables de permutation et de substitution pour le STA	225
C.6	Codes EA	226
C.7	Codes de TokenCarrierType	226
C.8	Instances de MeterFunctionObject / spécifications d'accompagnement	226
C.9	TariffIndex	226
C.10	Certification de conformité à la STS	227
C.10.1	Services de certification IEC	227
C.10.2	Produits	227
C.10.3	Autorité de certification	227
C.11	Options d'approvisionnement pour les utilisateurs de systèmes conformes à la STS	227
C.12	Gestion du passage par zéro des TID	231
C.12.1	Introduction	231
C.12.2	Vue d'ensemble	231
C.12.3	Analyse d'impact	233
C.12.4	Dates de référence	234
C.12.5	Mise en œuvre	234
Bibliographie	237

Figure 1 – Diagramme fonctionnel en blocs d'un compteur à paiement générique en une seule partie 130

Figure 2 – STS modélisée comme une pile protocolaire OSI réduite à 2 couches 131

Figure 3 – Flux de données du POSApplicationProcess vers le TokenCarrier	133
Figure 4 – Flux de données du TokenCarrier vers le MeterApplicationProcess.....	135
Figure 5 – Composition d'un numéro de référence de transaction ISO	136
Figure 6 – Transposition des 2 bits de Class.....	156
Figure 7 – Fonction TCDUGeneration pour les jetons de Class 0, 1 et 2	158
Figure 8 – Fonction TCDUGeneration pour le jeton Set1stSectionDecoderKey	160
Figure 9 – Fonction TCDUGeneration pour le jeton Set2ndSectionDecoderKey	162
Figure 10 – Changements de DecoderKey – diagramme d'états.....	169
Figure 11 – DecoderKeyGenerationAlgorithm01.....	175
Figure 12 – DecoderKeyGenerationAlgorithm02.....	176
Figure 13 – DecoderKeyGenerationAlgorithm03.....	177
Figure 14 – STA: EncryptionAlgorithm07.....	178
Figure 15 – Processus de substitution de chiffrement STA.....	179
Figure 16 – Processus de permutation de chiffrement STA.....	179
Figure 17 – Processus de rotation de DecoderKey de chiffrement STA.....	180
Figure 18 – Exemple pratique de chiffrement STA pour un jeton de TransferCredit.....	182
Figure 19 – DEA: EncryptionAlgorithm09	183
Figure 20 – Fonction d'APDUExtraction	187
Figure 21 – Extraction des 2 bits de Class	187
Figure 22 – DecryptionAlgorithm07 STA	191
Figure 23 – Processus de permutation de déchiffrement STA	192
Figure 24 – Processus de substitution de déchiffrement STA.....	193
Figure 25 – Processus de rotation de DecoderKey de déchiffrement STA	194
Figure 26 – Exemple pratique de déchiffrement STA pour un jeton de TransferCredit.....	196
Figure 27 – DEA DecryptionAlgorithm09	196
Figure A.1 – KeyManagementSystem et relations interactives entres des entités.....	214
Figure B.1 – Entités et identificateurs déployés dans un système conforme à la STS.....	218
Figure C.1 – Vue d'ensemble du système	232
Tableau 1 – Éléments de données dans l'APDU.....	137
Tableau 2 – Éléments de données dans l>IDRecord	138
Tableau 3 – Éléments de données dans le MeterPAN	138
Tableau 4 – Éléments de données dans l'IAIN / DRN.....	139
Tableau 5 – Types de support de jeton	140
Tableau 6 – Codes de DKGA	140
Tableau 7 – Codes EA.....	141
Tableau 8 – Types de SGC et types de clés.....	141
Tableau 9 – Codes de DOE pour l'année	143
Tableau 10 – Codes de DOE pour le mois	143
Tableau 11 – Format de définition de jeton	143
Tableau 12 – Éléments de données utilisés dans des jetons.....	147
Tableau 13 – Classes de jetons	148
Tableau 14 – Sous-classes de jetons.....	149

Tableau 15 – Exemples de calcul de TID	150
Tableau 16 – Unités de mesure pour l'électricité	151
Tableau 17 – Unités de mesure pour d'autres applications	152
Tableau 18 – Allocations des bits pour le TransferAmount	152
Tableau 19 – Erreur maximale d'arrondi	152
Tableau 20 – Exemples de valeurs de TransferAmount pour le transfert de crédit	153
Tableau 21 – Exemple de calcul de CRC	153
Tableau 22 – Valeurs admissibles du champ Control	154
Tableau 23 – Sélection du registre à vider	155
Tableau 24 – Classification des VendingKey (clés de vente)	164
Tableau 25 – Classification des DecoderKey (clés de décodeur)	165
Tableau 26 – Relations autorisées entre les types de clés de décodeur	170
Tableau 27 – Définition du PANBlock	172
Tableau 28 – Éléments de données dans le PANBlock	172
Tableau 29 – Définition du CONTROLBlock	172
Tableau 30 – Éléments de données dans le CONTROLBlock	173
Tableau 31 – Plage des valeurs applicables pour les numéros de référence de décodeur	173
Tableau 32 – Liste des valeurs applicables pour les codes de groupe d'alimentation	174
Tableau 33 – Tables de substitution d'échantillons	179
Tableau 34 – Tableau de permutation d'échantillons	179
Tableau 35 – Éléments de données dans l'APDU	184
Tableau 36 – Valeurs possibles de l'AuthenticationResult	184
Tableau 37 – Valeurs possibles du ValidationResult	185
Tableau 38 – Valeurs possibles du TokenResult	185
Tableau 39 – Valeurs stockées dans le DKR	190
Tableau 40 – Tableau de permutation d'échantillons	192
Tableau 41 – Tables de substitution d'échantillons	193
Tableau 42 – Entités/services exigeant un service de maintenance	205
Tableau A.1 – Entités qui participent aux processus de KMS	214
Tableau A.2 – Processus entourant le compteur à paiement et la DecoderKey	214
Tableau A.3 – Processus entourant le CryptographicModule	215
Tableau A.4 – Processus entourant le SGC et la VendingKey	215
Tableau B.1 – Entités types déployées dans un système conforme à la STS	218
Tableau B.2 – Identificateurs associés aux entités dans un système conforme à la STS	220
Tableau C.1 – Éléments de données associés à un SGC	223
Tableau C.2 – Éléments de données associés au CryptographicModule	224
Tableau C.3 – Éléments qu'il convient de noter dans les ordres d'achat et les soumissions d'offres	227

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.

La Norme internationale IEC 62055-41 a été établie par le comité d'études 13 de l'IEC: Mesure de l'énergie électrique, contrôle des tarifs et de la charge.

Cette deuxième édition annule et remplace la première édition, parue en 2007. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- Le jeton de Classe 2 est étendu de façon à inclure le transfert de crédit pour le gaz et l'eau et les extensions associées dans les jetons display/test.
- MfrCode est étendu de 2 à 4 chiffres.
- Trois dates de référence d'identificateur de jeton sont définies pour des changements de clé plus fréquents avec des procédures de passage par zéro de l'identificateur de jeton (TID).

- Un code de bonnes pratiques pour la gestion des changements de clé par passage par zéro de l'identificateur de jeton (TID) en association avec l'ensemble révisé de dates de référence.
- Des clarifications et des exemples supplémentaires ont été introduits.

Le texte de cette norme est issu des documents suivants:

CDV	Rapport de vote
13/1530/CDV	13/1553/RVC

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 cette publication 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 à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

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 de la présente Norme, l'IEC 62055 comprenait les parties suivantes, sous le titre général, *Équipements de comptage de l'électricité – Systèmes de paiement*:

- Partie 21: Cadre pour la normalisation
- 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 51: Spécification de transfert normalisé – Protocole de couche physique pour supports de jeton à carte magnétique et numérique unidirectionnel
- Partie 52: Spécification de transfert normalisé – Protocole de couche physique pour support de jeton virtuel bidirectionnel pour raccordement local direct

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

La Spécification de transfert normalisé (Standard transfer specification - STS) est un protocole de message sécurisé qui permet de transporter des informations entre des équipements de point de vente (Point of sale - POS) et des compteurs de paiement. Elle permet plusieurs types de message 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 pour permettre 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 dans 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 nouvelles études 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 "MaximumPowerLimit" 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 "Load Switch" 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 la présente Norme 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.11.

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

La publication de l'IEC 62055-41 Éd. 1 en mai 2007 a conduit à son adoption rapide comme la norme globale préférentielle pour les compteurs de prépaiement dans plusieurs pays membres de l'IEC et dans une majorité de pays membres affiliés à l'IEC. Des compteurs d'électricité pour le 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 système distributeur, d'agents de vente, d'institutions bancaires et d'industries adjacentes. Les intérêts pluripartites sont servis par la STS Association comportant plus de 130 organisations sises dans plus de 24 pays. L'interopérabilité et la conformité au Système 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 de prépaiement en Afrique - par l'intermédiaire d'une liaison de type D du groupe de travail WG 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 35 millions de compteurs exploités par 400 entreprises de distribution dans 30 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.

Le succès global a engendré un besoin pressant d'étendre la gamme des éléments numériques contenus dans les tableaux de l'IEC 62055-41. En particulier, il est nécessaire d'étendre la plage des numéros de constructeurs au-delà des 99 numéros initialement fournis. En outre, l'application de la norme a été étendue pour permettre des systèmes d'énergies multiples comprenant des compteurs de gaz et d'eau. En conséquence, le besoin existe d'assurer que le contenu de l'IEC 62055-41 est maintenu pour permettre cette croissance du marché et ces extensions à énergies multiples.

Plusieurs corrections et clarifications sont également requises pour réactualiser l'Édition 1 par rapport à la pratique courante. Cela avait été envisagé par le groupe de travail WG 15 du CE 13 lors de sa réunion du 20 septembre 2012 à Londres. Selon l'accord conclu, il convient de réviser l'IEC 62055-41.

Seules les révisions requises les plus urgentes ont été incorporées dans l'Édition 2 en raison des contraintes de temps, mais il est prévu que l'Édition 3 envisage des révisions supplémentaires afin d'incorporer les fonctionnalités suivantes:

- Transfert de devises
- Sécurité renforcée allant de pair avec les pratiques industrielles contemporaines
- Fonctions complexes pleinement harmonisées avec la suite DLMS/COSEM (Device Language Message Specification/Companion Specification for Energy Metering, à savoir "Spécification des messages de langage de dispositif/Spécification d'accompagnement pour le comptage d'énergie
- Système de gestion décentralisée de clés avec une architecture distribuée
- Suite d'essais de certification de conformité conjointement avec la Méthode OC de l'IECEE

La Commission Electrotechnique 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'identificateur de jeton réservé spécial 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>) maintiennent des bases de données, consultables en ligne, des droits de propriété pertinents à leurs normes. Les utilisateurs sont encouragés à consulter ces bases de données pour obtenir l'information la plus récente 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 IEC 62055-41 [Voir Article C.1]. L'IEC ne prend pas position quant à la preuve, la validité et la portée de ces services 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: sts@vdw.co.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. À l'origine, elle est destinée à être appliquée avec les compteurs à paiement d'électricité simple tarif utilisant des jetons basés sur l'énergie. Mais 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 jeton;
- 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 clé conforme à la STS;
- des lignes directrices pour un système de gestion de clé;
- des entités et des identificateurs utilisés dans un système STS;
- le code de bonnes pratiques pour la gestion des changements de clé par passage par 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 tenus d'accepter les jetons conformes à la STS et aussi par les constructeurs de systèmes POS tenus de produire des jetons conformes à la STS. Elle est à lire conjointement avec la série IEC 62055-5x.

Les produits conformes à la STS sont tenus de se conformer à des parties sélectives de la présente Norme internationale seulement, celles-ci sont l'objet du contrat d'achat (voir aussi Article C.11).

NOTE Bien qu'elle ait été mise au point pour les systèmes de paiement pour l'électricité, la norme prend 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 sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 60050 (toutes les parties), *Vocabulaire Electrotechnique International* (disponible à <<http://www.electropedia.org>>)

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

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

IEC 62055-31:2005, *Équipements 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 7812-1:2006, *Identification cards -- Identification of issuers -- Part 1: Numbering system* (disponible en anglais seulement)

ISO/IEC 7812-2:2007, *Identification cards -- Identification of issuers -- Part 2: Application and registration procedures* (disponible en anglais seulement)

ANSI X3.92-1981, *American National Standard Data Encryption Algorithm, American National Standards Institute – Data Encryption Algorithm* (disponible en anglais seulement)

FIPS PUB 46-3:1999, *Federal Information Processing Standards Publication – Data Encryption Standard* (disponible en anglais seulement)