

INTERNATIONAL STANDARD



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2018 IEC, Geneva, Switzerland

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

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

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

About the IEC

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

About IEC publications

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

IEC Catalogue - webstore.iec.ch/catalogue

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

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

IEC Glossary - std.iec.ch/glossary

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

IEC Customer Service Centre - webstore.iec.ch/csc

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

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 978-2-8322-5556-8

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

CONTENTS

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

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

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

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

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

~~Figure~~	~~TCDUGeneration function for Set2ndSectionDecoderKey token~~	~~21~~
~~Figure~~	~~DecoderKeyGenerationAlgorithm03~~	~~22~~
~~Figure~~	~~DEA: EncryptionAlgorithm09~~	~~23~~
~~Figure~~	~~DEA DecryptionAlgorithm09~~	~~24~~
Figure 1	Functional block diagram of a generic single-part device payment meter.....	21
Figure 2	STS modelled as a 2-layer collapsed OSI protocol stack	22
Figure 3	Dataflow from the POSApplicationProcess to the TokenCarrier	23
Figure 4	Dataflow from the TokenCarrier to the MeterApplicationProcess	24
Figure 5	~~ISO~~ Composition of transaction reference number	25
Figure 6	Transposition of the 2 Class bits	50
Figure 7	TCDUGeneration function for Class 0, 1 and 2 tokens	51
Figure 8	TCDUGeneration function for key change tokens	52
Figure 9	DecoderKey changes – state diagram	61
Figure 10	DecoderKeyGenerationAlgorithm01.....	67
Figure 11	DecoderKeyGenerationAlgorithm02.....	68
Figure 12	STA: EncryptionAlgorithm07.....	71
Figure 13	STA encryption substitution process.....	72
Figure 14	STA encryption permutation process	73
Figure 15	STA encryption DecoderKey rotation process.....	73
Figure 16	STA encryption worked example for TransferCredit token	74
Figure 17	MISTY1: EncryptionAlgorithm11	76
Figure 18	MISTY1 encryption worked example for TransferCredit token.....	77
Figure 19	APDUExtraction function	80
Figure 20	Extraction of the 2 Class bits.....	81
Figure 21	STA DecryptionAlgorithm07	84
Figure 22	STA decryption permutation process	84
Figure 23	STA decryption substitution process.....	85
Figure 24	STA decryption DecoderKey rotation process.....	86
Figure 25	STA decryption worked example for TransferCredit token	87
Figure 26	STA DecryptionAlgorithm11	88
Figure 27	MISTY1 decryption worked example for TransferCredit token.....	89
Figure A.1	KeyManagementSystem and interactive relationships between entities.....	104
Figure B.1	Entities and identifiers deployed in an STS-compliant system	108
Figure C.1	System overview	122
Table 1	Data elements in the APDU	26
Table 2	Data elements in the IDRecord	26
Table 3	Data elements in the MeterPAN.....	27
Table 4	Data elements in the IAIN / DRN	28

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

FOREWORD

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

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

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

- currency transfer tokens for electricity, water, gas and time metering;
- finer resolution for gas and time credit transfer;
- common code PAN for 2 and 4 digit manufacturer codes;
- reserved MfrCode values for certification and testing purposes;
- provision for DLMS/COSEM as a virtual token carrier type;
- addition of DKGA04, an advanced key derivation function from 160-bit VendingKey;
- withdrawal of DES for EA09 and TDES for DKGA03 cryptographic algorithms, but DES for DKGA02 remains in use;
- addition of MISTY1 cryptographic algorithm using a 128-bit DecoderKey with supporting key change tokens;
- transfer of SGC values to the meter via key change tokens;
- revision of the test/display token requirements;
- revision of the KMS to reflect current best practice;
- revision of the TID roll over management guidelines;
- definition of BaseDate is referenced to Coordinated Universal Time;
- disassociation of IIN from the ISO standard definition;
- various clarifications and enhancements to support the above.

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

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

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

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

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

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

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

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

INTRODUCTION

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

Part 21: Framework for standardization

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

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

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

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

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

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

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

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

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

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

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

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

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

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

majority of IEC affiliate member countries. Prepayment electricity meters and their associated Payment Systems are now produced, operated and maintained by an ecosystem of utilities, meter manufacturers, meter operators, vending system providers, vending agents, banking institutions and adjacent industries. Multi-stakeholder interests are served by the STS Association comprising of more than ~~130~~ 150 organisations located in over ~~24~~ 35 countries. Interoperability and conformance to the Standard Transfer-~~System~~ Specification (STS) are guaranteed by Conformance test specifications developed and administered by the STS Association. A full list of the STS Association services can be found at <http://www.sts.org.za>.

Developed originally for prepayment electricity meters in Africa – via an IEC TC13 WG15 D-type liaison with the STS Association – this IEC standard now serves more users in Asia than Africa, with a total of approximately ~~35~~ 50 million meters operated by ~~400~~ 500 utilities in ~~30~~ 94 countries. Management of the technology has been administered by the STS Association in fulfilment of its role as the IEC appointed Registration Authority.

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

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

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

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

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

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

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

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

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

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

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

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

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

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning encryption key management and the stack of protocols on which the present International Standard IEC 62055-41 is based [see Clause C.1]. The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

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

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

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

1 Scope

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

It specifies:

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

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms, definitions, abbreviated terms, notation and terminology

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ~~IEC 60050~~, IEC TR 62051 and IEC 62055-31 as well as the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

NOTE Where there is a difference between the definitions in this document and those contained in other referenced IEC standards, then those defined in this document take precedence.

The term “meter” is used interchangeably with “payment meter”, “prepayment meter” and “decoder”, where the decoder is a sub-part of an electricity payment meter or of a multi-part device payment meter.

The term “POS” is used synonymously with “CIS”, “MIS” and “HHU” in the sense that tokens may also be generated by, and transferred between these entities and the payment meter.

The term “utility” is used to signify the supplier of the service in a general sense. In the liberalized markets the actual contracting party acting as the “supplier” of the service to the consumer may not be the traditional utility as such, but may be a third party service provider.

3.1.1

companion specification

specification managed by the STS Association, which defines a specific instance of a MeterFunctionObject

SEE: 5.5 and Clause C.9.

3.1.2

decoder

part of the TokenCarrierToMeterInterface of a payment meter that performs the functions of the application layer protocol and which allows token-based transactions to take place between a POS and the payment meter

3.1.3

meter serial number

number that is associated with the metrological part of the payment meter

Note 1 to entry: In a single-part device payment meter the DRN and meter serial number may be synonymous, while in a multi-part device payment meter they may be different.

3.1.4

token

subset of data elements, containing an instruction and information that is present in the APDU of the Application Layer of the POSToTokenCarrierInterface, and which is also transferred to the payment meter by means of a token carrier (the converse is also true in the case of a token being sent from the payment meter to the POS)

3.1.5

token carrier

medium that is used in the Physical Layer of the POSToTokenCarrierInterface, onto which a token is modulated or encoded, and which serves to carry a token from the point where it is generated to the remote payment meter, where it is received

3.1.6

one-way token carrier system

payment metering system, which employs token carriers that transfer information in one direction only – from the POS to the payment meter

3.1.7

token-based transaction

processing of any token by the payment meter that has material effect on the amount, value or quality of service to be delivered to the consumer under control of the payment meter (in terms of current practice this means tokens of Class 0 and Class 2)

3.1.8

supported

ability to perform a defined function

Note 1 to entry: If a supported function is disabled, it remains supported.

3.1.9

base currency

particular currency denomination for the country that the receiving meter account is operating in, as defined in ISO 4217

EXAMPLES USD/840, EUR/978, GBP/826, ZAR/710.

3.2 Abbreviated terms

ANSI American National Standards Institute

APDU ApplicationProtocolDataUnit

BDT BaseDate

CA CertificationAuthority

CC CountryCode

CERT Certified public key

CIS Customer Information System

CM CryptographicModule

~~CMAC CryptographicModuleAuthenticationCode~~

CMID CryptographicModuleIdentifier

COP Code of practice

COSEM Companion Specification for Energy Metering

CRC CyclicRedundancyCodeCheck

DAC DeviceAuthenticationCode

DCTK DecoderCommonTransferKey

DD Discretionary Data

DDTK DecoderDefaultTransferKey

DEA Data Encryption Algorithm

DES Data Encryption Standard

DITK DecoderInitializationTransferKey

DK DecoderKey

DKGA DecoderKeyGenerationAlgorithm

DKR DecoderKeyRegister

DLMS Distribution Line Message Specification

DOE DateOfExpiry

DRN DecoderReferenceNumber [known as a “meter number” in systems in use prior to the development of this document]

DSN DecoderSerialNumber

DUTK DecoderUniqueTransferKey

EA EncryptionAlgorithm

ECB Electronic Code Book

ETX ASCII End of Text character

FAC FirmwareAuthenticationCode

FIPS Federal Information Processing Standards

FOIN FunctionObjectIdentificationNumber

FS FieldSeparator

GPRS General Packet Radio Service

GSM Global System For Mobile Communications

HHU	HandHeldUnit
HMAC	Hash Message Authentication Code
IAIN	IndividualAccountIdentificationNumber
ID	Identification; Identifier
IIN	IssuerIdentificationNumber
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
~~ISO BIN~~	~~Replaced by IIN~~
KCT	KeyChangeToken
KDF	Key Derivation Function
KEK	KeyExchangeKey
KEN	KeyExpiryNumber
KLF	KeyLoadFile
KMC	KeyManagementCentre
KMI	KeyManagementInfrastructure
KMS	KeyManagementSystem
KRN	KeyRevisionNumber
KT	KeyType
LAN	Local Area Network
LRC	LongitudinalRedundancyCheck
MFO	MeterFunctionObject
Mfr	Manufacturer
MII	MajorIndustryIdentifier
MIS	Management Information System
MPL	MaximumPowerLimit
MPPUL	MaximumPhasePowerUnbalanceLimit
NIST	National Institute of Standards and Technology
NKHO	NewKeyHighOrder bits
NKLO	NewKeyLowOrder bits
NWIP	New Work Item Proposal
OSI	Open Systems Interconnection
PAN	PrimaryAccountNumber
PLC	Power Line Carrier
POS	PointOfSale
PRN	Printer
PSTN	Public Switched Telephone Network
RND	RandomNumber
RO	Roll over
SG	SupplyGroup
SGC	SupplyGroupCode
SHA	Secure Hash Algorithm
STA	Standard Transfer Algorithm
STS	Standard Transfer Specification

STSA	Standard Transfer Specification Association
STX	ASCII Start of Text character
TCDU	TokenCarrierDataUnit
TCT	TokenCarrierType
TDEA	Triple Data Encryption Algorithm
TI	TariffIndex
TID	TokenIdentifier
UC	UtilityCode
VCDK	VendingCommon ~~DES~~ DerivationKey
VDDK	VendingDefault ~~DES~~ DerivationKey
VK	VendingKey
VUDK	VendingUnique ~~DES~~ DerivationKey
WAN	Wide Area Network
XOR	Exclusive Or (logical)

3.3 Notation and terminology

Throughout this document the following rules are observed regarding the naming of terms:

- entity names, data element names, function names and process names are treated as generic object classes and are given names in terms of phrases in which the words are capitalized and joined without spaces. Examples are: SupplyGroupCode as a data element name, EncryptionAlgorithm07 as a function name and TransferCredit as a process name (see note);
- direct (specific) reference to a named class of object uses the capitalized form, while general (non-specific) reference uses the conventional text i.e. lower case form with spaces. An example of a direct reference is: “The SupplyGroupCode is linked to a group of meters”, while an example of a general reference is: “A supply group code links to a vending key”;
- other terms use the generally accepted abbreviated forms like PSTN for Public Switched Telephone Network.

NOTE The notation used for naming of objects has been aligned with the so called “camel-notation” used in the common information model (CIM) standards prepared by IEC TC 57, in order to facilitate future harmonization and integration of payment system standards with the CIM standards.

4 Numbering conventions

In this document, the representation of numbers in binary strings uses the convention that the least significant bit is to the right, and the most significant bit is to the left.

Numbering of bit positions start with bit position 0, which corresponds to the least significant bit of a binary number.

Numbers are generally in decimal format, unless otherwise indicated. Any digit without an indicator signifies decimal format.

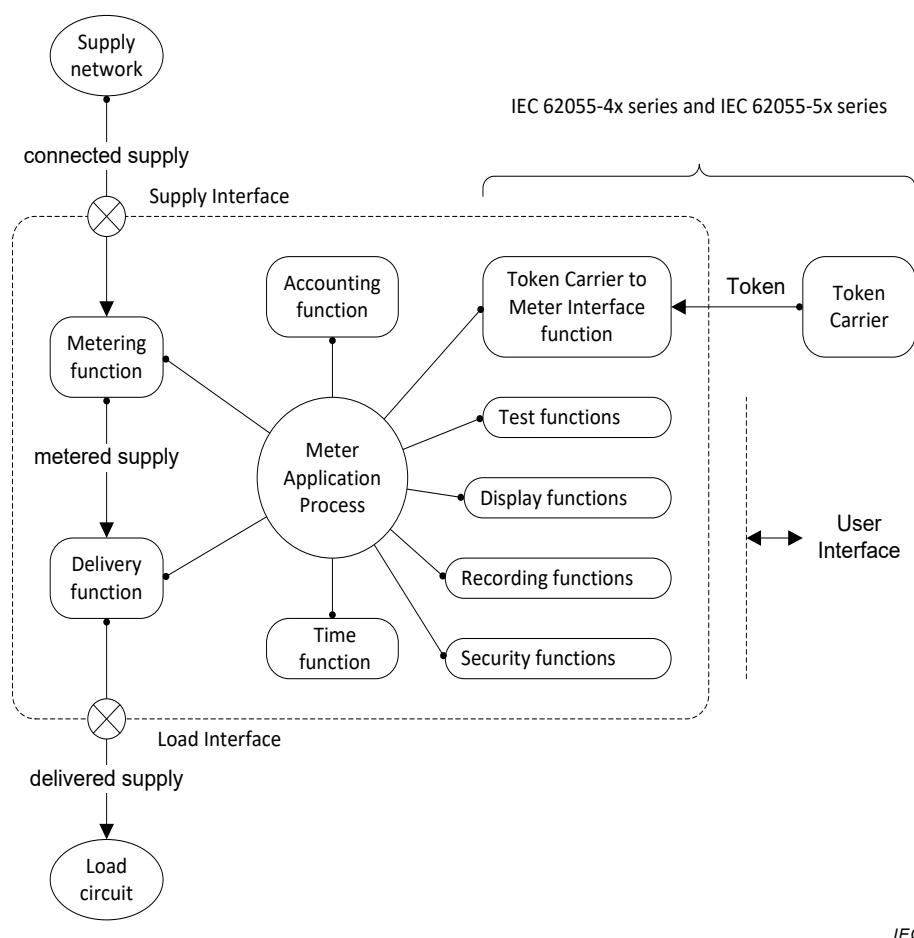
Binary digit values range from 0 to 1.

Decimal digit values range from 0 to 9.

Hexadecimal digit values range from 0 to 9, A to F and are indicated by “hex”.

5 Reference model for the standard transfer specification

5.1 Generic payment meter functional reference diagram



IEC

Figure 1 – Functional block diagram of a generic single-part device payment meter

In a single-part device payment meter all the essential functions are located in a single enclosure as depicted in Figure 1 above, ~~in which case the decoder is integral with the metering function and the DRN could thus optionally be synonymous with the meter serial number~~ while in a multi-device payment meter it is possible for the TokenCarrierToMeterInterface to be located in a separate enclosure.

The IEC 62055-4x series primarily deals with the application layer protocol and IEC 62055-5x series with the physical layer protocol of the TokenCarrierToMeterInterface. The TokenCarrier is included in the Physical Layer.

In this document the Decoder (see Clause 3) is defined as that part of the payment meter where the Application Layer functions of the TokenCarrierToMeterInterface are ~~located~~ hosted and it is thus allocated a DRN (see 6.1.2.3).

NOTE MeterFunctionObjects are further discussed in 5.5.

~~In a multi-part payment meter it is possible for the TokenCarrierToMeterInterface to be located in a separate enclosure from that of the metering function for example, which may well be a standalone meter in its own right and having its own meter serial number. In this case, the DRN would not be the same as the meter serial number, but would be distinctly different and would thus be marked on the enclosure containing the decoder.~~

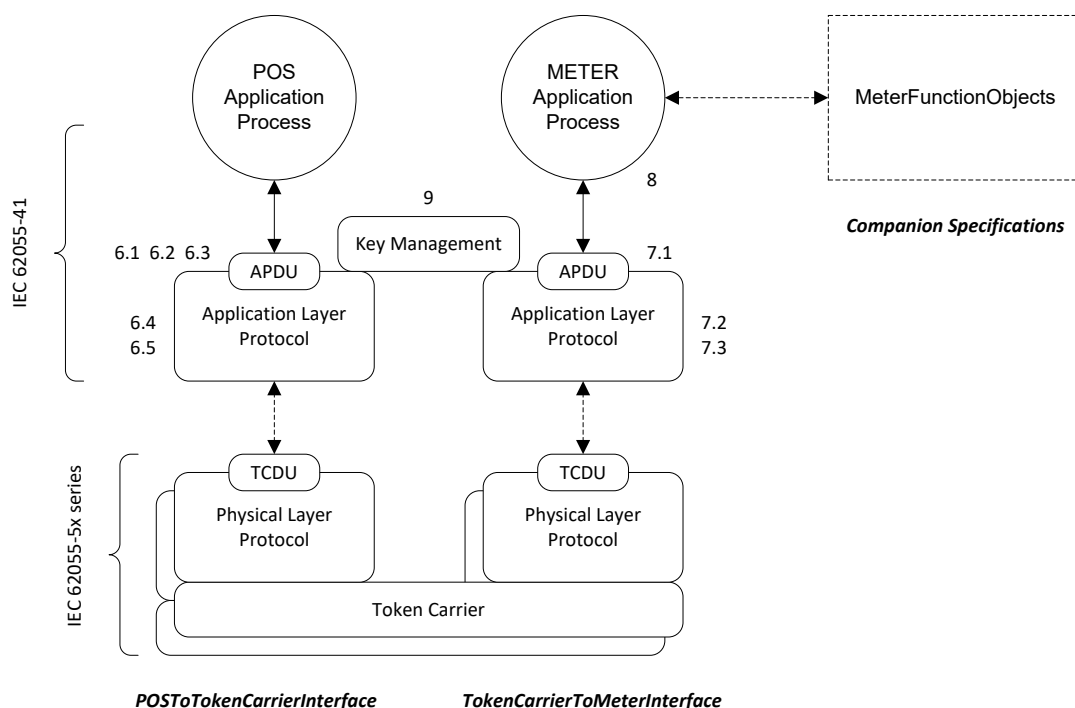
In all cases, there shall only be one Application Layer implementation, thus there shall be only one DRN associated with a payment meter, whether it is a single or multi-part device.

implementation, even though there may also be more than one Physical Layer implementation in the same payment meter.

~~It is also possible that the Application Layer functions and the Physical Layer functions are located in separate enclosures, in which case, the marking (see 8.3) of the DRN and the EA code is applied to that part that contains the physical TokenCarrier connection point. This may be a cable or modem connector for a virtual token carrier, a keypad for a numeric token carrier or a magnetic card reader for magnetic card token carrier for example (see also 5.2 for more examples of token carriers).~~

For a more complete description of payment meter function classes see IEC TR 62055-21.

5.2 STS protocol reference model



IEC

Key

APDU ApplicationProtocolDataUnit; data interface to the application layer protocol

TCDU TokenCarrierDataUnit; data interface to the physical layer protocol

Relevant (sub)clause number references in this document are indicated adjacent to each box.

Figure 2 – STS modelled as a 2-layer collapsed OSI protocol stack

The STS is a secure data transfer protocol between a POS and a payment meter using a token carrier as the transfer medium. The application layer protocol deals with tokens and encryption processes and functions, while the physical layer protocol deals with the actual encoding of token data onto a token carrier (see Figure 2).

Examples of physically transportable token carrier devices are: numeric, magnetic cards, memory cards and memory keys. Examples of virtual token carriers are: PSTN modem, ISDN modem, GSM modem, GPRS modem, Radio modem, PLC modem, Infra-red, LAN and WAN connections and direct local connection. These are defined in the IEC 62055-5x series.

It shall be noted that although the model primarily depicts a POS to token carrier to payment meter protocol, the same protocol is equally applicable to any other device that requires communicating with the payment meter, for example CIS, MIS or portable HHU.

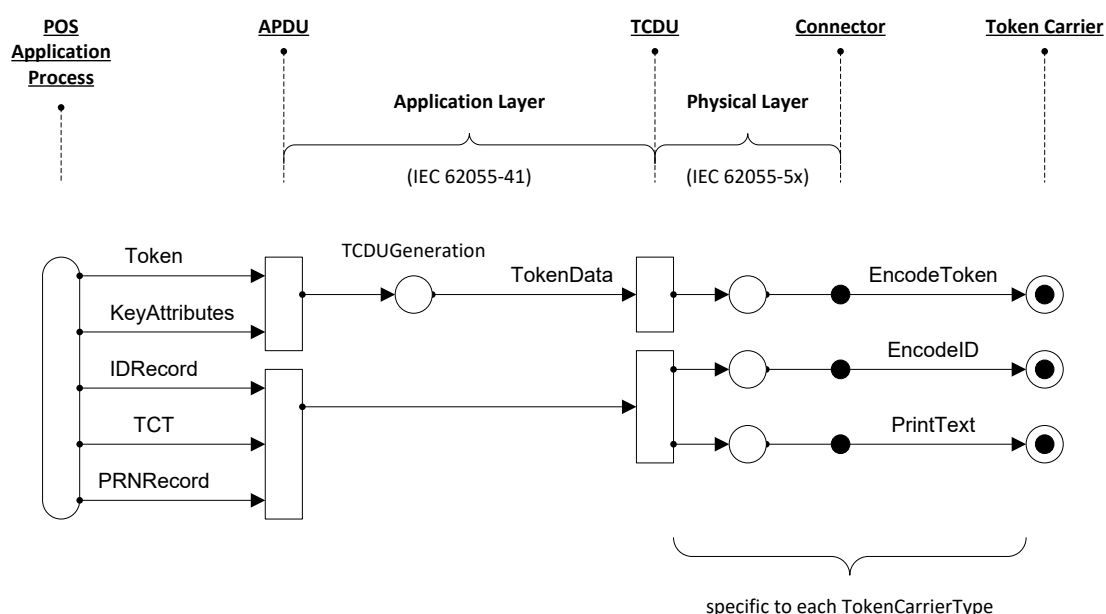
Although a collapsed 2-layered OSI architecture is followed in this document, it does not preclude future expansion to include more layers should the need arise or for the implementer to interpose additional layers between the two shown in this model.

The APDU is the data interface to the application layer protocol, specified in IEC 62055-41 and the TCDU is the data interface to the physical layer protocol, specified in the IEC 62055-5x series.

The STS in this document defines a one-way data transfer protocol (i.e. from POS to payment meter), although the reference model allows equally for a two-way transfer protocol, which may be a requirement in a future revision of this document.

5.3 Dataflow from the POSApplicationProcess to the TokenCarrier

The flow of data from the POSApplicationProcess to the TokenCarrier is shown in Figure 3.



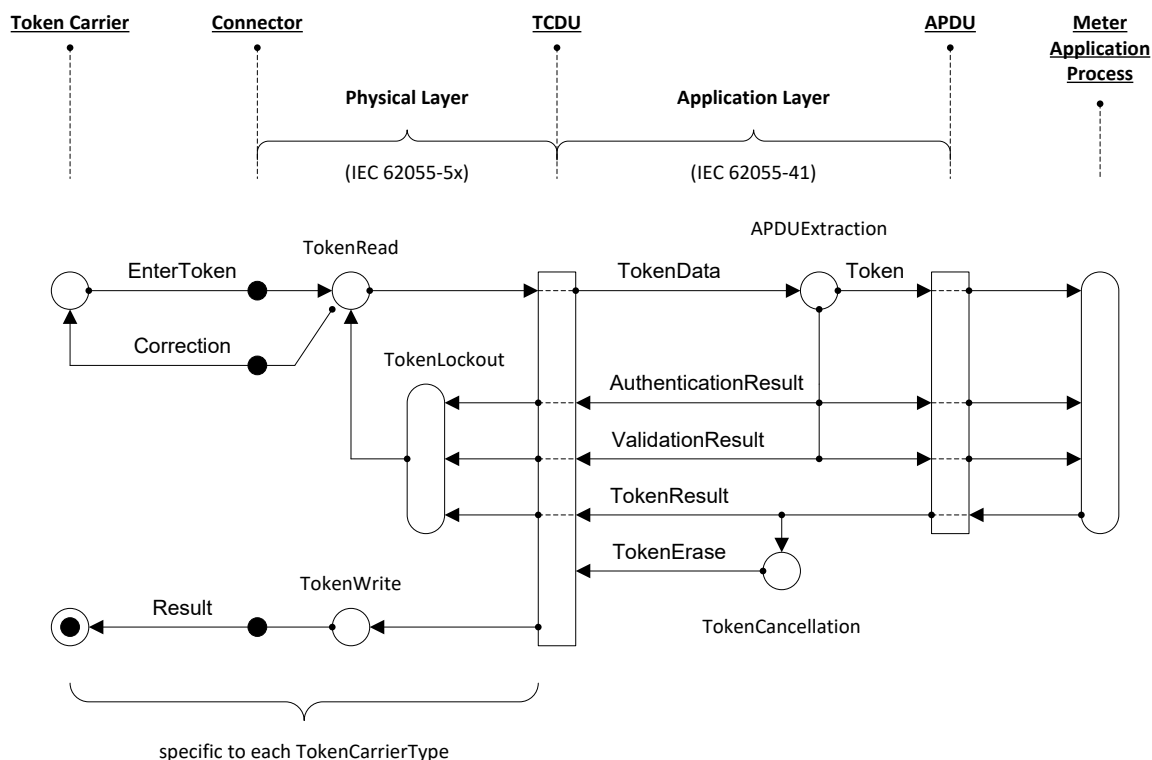
IEC

Figure 3 – Dataflow from the POSApplicationProcess to the TokenCarrier

The POSApplicationProcess presents the token to the APDU together with the KeyAttributes of the DecoderKey that is to be used for encrypting the token. The application layer protocol generates the DecoderKey, encrypts the token and presents the resultant TokenData in the TCDU. The physical layer protocol encodes the TokenData onto the TokenCarrier. Optionally, payment meter identification data may also be encoded onto the TokenCarrier (see 5.2.4 in IEC 62055-51:2007 for example) as well as printed text onto the outside surface (see 5.1.5 in IEC 62055-51:2007 for example). This part of the process essentially ends with the encoding of data onto the TokenCarrier, after which the TokenCarrier is transported to the payment meter (usually by the customer), where it is entered into the payment meter via the TokenCarrierInterface.

5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess

The flow of data from the TokenCarrier to the MeterApplicationProcess is shown in Figure 4.



IEC

Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess

The token entry process from the TokenCarrier varies according to the TCT. The nature of the connector will similarly vary according to the TCT, an example of which may be a keypad or a magnetic card reader device supporting one-way token carriers as specified in IEC 62055-51.

NOTE Where other types of connectors ~~would be~~ are required to support other types of token carriers such as a memory key reader device or a plug-in connector from a hand-held unit acting as a virtual token carrier, ~~then~~ such token carriers ~~might~~ shall be specified in additional parts of IEC 62055-5x in the future.

The physical layer protocol reads the token data being entered and provides immediate corrective feedback to the user (see 6.3 in IEC 62055-51:2007 for example). The entered token data is presented in the TCDU, from where the application layer protocol extracts the token by appropriate decryption, validation and authentication, the results of which are presented to the MeterApplicationProcess in the APDU. After processing and executing the instruction from the token, the MeterApplicationProcess indicates the result in the APDU for the application layer protocol to take further action. This normally causes the cancellation of the TID and the giving of the instruction, via the TCDU, to the physical layer protocol to complete the token entry process by erasure of the token data (if appropriate) or by writing of other relevant data back onto the TokenCarrier as may be appropriate.

For certain TokenCarrier types (for example a high speed virtual token carrier) the physical layer protocol may employ a token entry lockout function to protect the payment meter from fraud attempts. Typically, such a lockout function would slow down the effective rate, at which tokens may be entered via the particular token carrier interface (see 6.6.7 of IEC 62055-52:2008 for example).

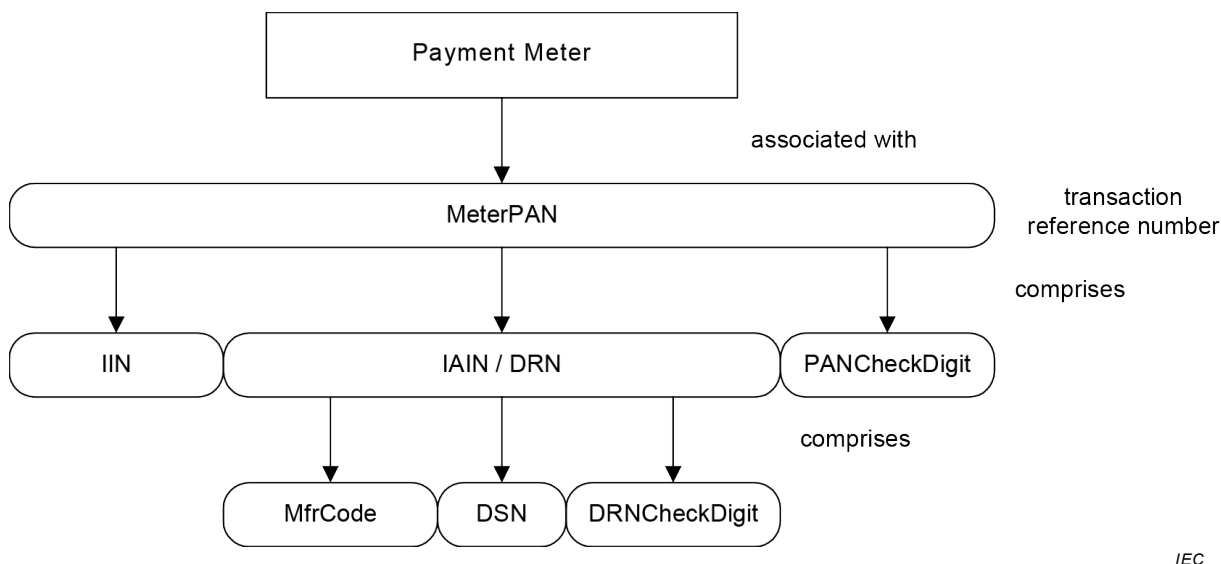
5.5 MeterFunctionObjects / companion specifications

With reference to Figure 1 it can be seen that the TokenCarrierToMeterInterface, which also includes the TokenCarrier, is dealt with in the IEC 62055-4x and IEC 62055-5x series.

remaining MeterFunctionObjects shown in the diagram are defined in companion specifications and are not normative to this document.

Companion specifications (see Figure 2) are under the administrative control (see Clause C.9) of the STS Association and serve the purpose of defining functionality of a payment meter in a standardized way, using an object-oriented approach.

5.6 ~~ISO~~ Transaction reference numbers



IEC

Figure 5 – Composition of ~~ISO~~ transaction reference number

The ~~ISO~~ transaction reference number comprises the data elements and their relationships as shown in Figure 5.

A token-based transaction (see Clause 3) constitutes a financial activity that needs to be dealt with in accordance with standard financial practices.

The PrimaryAccountNumber (PAN) ~~as defined by ISO/IEC 7812-1~~ serves to tag transaction records, messages, requests, authorizations and notifications, in which both transacting parties are uniquely identifiable.

A payment meter is thus uniquely associated with a MeterPAN, being a composite number comprising of IIN and IAIN / DRN, which in turn comprises MfrCode and DSN (see 6.1.2).

6 POSToTokenCarrierInterface application layer protocol

6.1 APDU: ApplicationProtocolDataUnit

6.1.1 Data elements in the APDU

The APDU is the data interface between the POSApplicationProcess and the application layer protocol and comprises the data elements given in Table 1.

Table 1 – Data elements in the APDU

Element	Context	Format	Reference
MeterPAN	~~ISO-compliant~~ Identification MeterPrimaryAccountNumber for the payment meter	18 digits	6.1.2
TCT	Directs which TokenCarrierType should be used in the physical layer protocol to carry the token to the payment meter	2 digits	6.1.3
DKGA	Directs which DecoderKeyGenerationAlgorithm is to be used for generating the DecoderKey	2 digits	6.1.4
EA	Directs which encryption algorithm is to be used for encrypting the token data	2 digits	6.1.5
SGC	Directs which SupplyGroupCode the payment meter is allocated to	6 digits	6.1.6
TI	Directs which TariffIndex the payment meter is linked to	2 digits	6.1.7
KRN	Directs which KeyRevisionNumber the DecoderKey is on (as inherited from VendingKey)	1 digit	6.1.8
KT	Directs which KeyType the DecoderKey is on	1 digit	6.1.9
KEN	A number associated with the VendingKey and a DecoderKey that determines the time period, during which the key will remain valid	8 bits	6.1.10
BaseDate	The starting date and time from which a TID is calculated	2 ASCII characters	6.1.12 6.5.3.6
Token	The actual token data that is to be transferred to the payment meter prior to encryption and processing	66 bits	6.2.1
IDRecord	Optional identification data intended to be encoded onto a payment meter ID card or onto a token carrier together with the token	35 digits	Table 2
PRNRecord	Optional print data intended to be printed at the same time as the coding of the token onto the TokenCarrier. Certain token carriers such as paper-based magnetic card devices allow printing to be done onto the card surface itself and this operation may be integrated with the magnetic card encoding device. The content and format is not specified and is left to each system to define according to its particular requirements	Undefined text	x

The optional IDRecord comprises the data elements given in Table 2.

Table 2 – Data elements in the IDRecord

Element	Context	Format	Reference
MeterPAN	~~ISO-compliant~~ Identification MeterPrimaryAccountNumber for the payment meter	18 digits	6.1.2
DOE	Optional expiry date for the identification data as encoded onto a payment meter ID card or token carrier (as an example, see IEC 62055-51)	4 digits	6.1.11
TCT	Indicates which TokenCarrierType is associated with this MeterPAN	2 digits	6.1.3
EA	Indicates which encryption algorithm is associated with this MeterPAN	2 digits	6.1.5
SGC	Indicates which SupplyGroupCode is associated with this MeterPAN	6 digits	6.1.6
TI	Indicates which TariffIndex is associated with this MeterPAN	2 digits	6.1.7
KRN	Indicates which KeyRevisionNumber is associated with this MeterPAN (as inherited from VendingKey)	1 digit	6.1.8

6.1.2 MeterPAN: MeterPrimaryAccountNumber

6.1.2.1 Data elements in the MeterPAN

The MeterPAN is a unique identification number for each STS-compliant payment meter. It comprises the 3 parts given in Table 3 ~~and is in accordance with the definition for the PAN (PrimaryAccountNumber) of ISO/IEC 7812-1.~~

Table 3 – Data elements in the MeterPAN

Element	Context	Format	Reference
IIN	IssuerIdentificationNumber	4/6 digits	6.1.2.2
IAIN / DRN	IndividualAccountIdentificationNumber / DecoderReferenceNumber	11/13 digits	6.1.2.3
PANCheckDigit	Result of a formula to check the integrity of the IIN and the IAIN	1 digit	6.1.2.4
NOTE The first digit of the IIN is the most significant digit of the 18-digit MeterPAN and the PANCheckDigit is the least significant digit.			

See also Annex C for Code of practice on managing this data element.

6.1.2.2 IIN: IssuerIdentificationNumber

The IIN is a unique 6/4-digit number that defines a domain, under which further IAIN values (i.e. DRN values) may be issued for use within this defined domain.

~~The original intent and purpose of the IIN was to be able to tag financial transactions in order to uniquely identify them and to route them to the appropriate transacting financial accounts. It was thus intended that the IIN be issued by the ISO under the registration scheme given in ISO/IEC 7812-1 and ISO/IEC 7812-2. However, this has proven to be impractical and the value 600727 for IIN has since become the de-facto standard for legacy systems utilising an 11-digit DRN.~~

~~It has subsequently become necessary to also make provision for 13-digit DRNs (as defined in 6.1.2.3.1) in which case the IIN shall be 0000 (four zeroes).~~

For 11-digit DRNs the IIN shall be 600727 and for 13digit DRNs the IIN shall be 0000.

See also C.4.2 on managing this data element.

6.1.2.3 IAIN: IndividualAccountIdentificationNumber/ DRN: DecoderReferenceNumber

6.1.2.3.1 Data elements in the IAIN / DRN

A unique DRN shall be allocated to the device that performs the application layer protocol in an STS-compliant payment meter.

NOTE In many systems, the decoder part is integral with the metering part and hence the DRN might be synonymous with the meter serial number.

The DRN is an 11/13-digit number comprising of the data elements given in Table 4.

Table 4 – Data elements in the IAIN / DRN

Element	Context	Format	Reference
MfrCode	A number to uniquely identify a payment meter manufacturer	2/4 digits	6.1.2.3.2
DSN	An eight digit serial number allocated by the manufacturer	8 digits	6.1.2.3.3
DRNCheckDigit	Check Digit; formula to check the integrity of the MfrCode and the DSN	1 digit	6.1.2.3.4
NOTE The MfrCode is the 2/4 most significant digits of the 11/13-digit DRN and the DRNCheckDigit is the least significant digit.			

MfrCode values shall always be right justified and left padded with 0's.

The DSN shall be right justified and left padded with 0 to a full 8-digit string.

6.1.2.3.2 MfrCode: ManufacturerCode

The MfrCode is a 2/4-digit number that shall be used to uniquely identify the manufacturer of the payment meter.

The STS Association provides a service for the allocation of MfrCode values to uniquely identify manufacturers in order to ensure interoperability of STS-compliant equipment.

MfrCode values 00 and 0100 are reserved for product certification test purposes and shall not be used in any production equipment.

See also C.4.3 on managing this data element.

6.1.2.3.3 DSN: DecoderSerialNumber

The DSN is a unique 8-digit serial number that is generated internally by the manufacturer. Each manufacturer is responsible for the uniqueness of the DSN with respect to his MfrCode.

See also C.4.4 on managing this data element.

6.1.2.3.4 DRNCheckDigit

The DRNCheckDigit is a single digit used to validate the integrity of the MfrCode and DSN values when being entered by hand or being read by machine. This is a modulus 10 check digit, calculated using the Luhn formula, as illustrated in Annex B of ISO/IEC 7812-1:2000 2006. It is calculated on the 10/12 preceding digits of the DRN generated through the concatenation of the MfrCode and the DSN values.

6.1.2.4 PANCheckDigit

The PANCheckDigit is a single digit used to validate the integrity of the IIN and the IAIN values when being entered by hand or being read by machine. The method used to calculate the PANCheckDigit value is given in 4.4 of ISO/IEC 7812-1:2000 2006 and is calculated on the preceding 17 digits of the MeterPAN generated through the concatenation of the IIN and the IAIN values.

6.1.3 TCT: TokenCarrierType

This is a 2-digit number used to uniquely identify the type of token carrier onto which the token should be encoded for transferring to the payment meter. The values for token carrier types are given in Table 5.

Table 5 – Token carrier types

Code	TokenCarrier	Comments
00	Reserved	For future assignment by the STS Association
01	Magnetic card	As defined in IEC 62055-51
02	Numeric	As defined in IEC 62055-51
03-06	Reserved	Legacy systems using proprietary token carrier technologies
07	Virtual Token Carrier (VTC07)	As defined in IEC 62055-52
08	DLMS_COSEM_VTC (VTC08)	Virtual token carrier type for transporting STS tokens over DLMS/COSEM
~~08~~ 09-99	Reserved	For future assignment by the STS Association
NOTE TCT08 is provisioned for a future standard.		

Values less than 10 shall be right justified and left padded with 0 (for example 01, 02-09).

6.1.4 DKGA: DecoderKeyGenerationAlgorithm

This is a 2-digit number used to uniquely identify which algorithm is to be used for generating the DecoderKey. The DKGA code values are given in Table 6.

Table 6 – DKGA codes

Code	DKG algorithm	Comments	Reference
00	Reserved	For future assignment by the STS Association	x
01	DKGA01	Limited number of early legacy STS-compliant payment meters. Superseded by DKGA02	6.5.3.3
02	DKGA02	System using 64-bit DES VendingKey ~~diversification~~ derivation	6.5.3.4
03	DKGA03	System using dual 64-bit DES VendingKey ~~diversification~~ derivation	6.5.3.5
04	DKGA04	System using KDF-HMAC-SHA-256 VendingKey derivation	6.5.3.6
~~04~~ 05-99	Reserved	For future assignment by the STS Association	x
DKGA02 is the algorithm to be used for current systems, subject to the criteria for DKGA01. ~~DKGA03 is the algorithm to be used for future systems requiring a higher level of security regarding protection of the VendingKey by "brute-force" attack.~~ ~~Introduction of DKGA03 should preferably coincide with the change from STA to DEA (EA code 07 to EA code 09). See also 6.1.5.~~ DKGA03 is deprecated and shall not be used for new products. DKGA04 shall be deployed in advance of, or in conjunction with, the introduction of meters using EA code 07 or code 11. See also 6.1.5.			

Values less than 10 shall be right justified and left padded with 0 (for example 01, 02-09).

6.1.5 EA: EncryptionAlgorithm

This is a 2-digit number used to uniquely identify which algorithm is to be used for encrypting the token data. The EA code values are given in Table 7.

Table 7 – EA codes

Code	EncryptionAlgorithm	Comments	Reference
00	Reserved	For future assignment by the STS Association	x
01-06	Reserved	Legacy proprietary systems	x
07	STA	Systems using the Standard Transfer Algorithm as defined in this document	6.5.4.1
08	Reserved	Legacy proprietary systems	x
09	DEA	Systems using the Data Encryption Algorithm as defined in ANSI X3.92	6.5.5
10	Reserved	Legacy proprietary systems	x
11	MISTY1	Systems using the Encryption Algorithm as defined in ISO/IEC 18033-3 as for MISTY1	6.5.6
~~11~~ 12-99	Reserved	For future assignment by the STS Association	x
~~It is recommended that the choice of EA code 09 be co-ordinated with the choice of DKGA03 in order to minimize the effect on existing systems in the installed base (see 6.1.4).~~ EA09 is deprecated and shall not be used for new products.			

Values less than 10 shall be right justified and left padded with 0. For example 01, 02-09.

6.1.6 SGC: SupplyGroupCode

This is a unique 6-digit decimal number allocated to a utility, which is registered within the KMS. It is used to uniquely identify a sub-group of payment meters within the supply or distribution domain of the utility. Each SupplyGroup has one or more VendingKeys associated with it ~~and hence~~. Each payment meter in the SupplyGroup has a ~~derived DecoderKey associated with it~~ DecoderKey derived from one of these VendingKeys. Token sales authorisation is thus controlled by selective distribution of such VendingKey and SGC to authorised token vendor agents operating POS services on behalf of utilities. SGC management and VendingKey management is completely under the control of the KMS and is subject to such Code of practice.

Values less than 6 decimal digits shall be right justified and left padded with 0. For example 000001, 000002.. 000009.

The SGC inherits its type from the KT attribute of the VendingKey (see 6.5.2.2.1), to which it is associated as shown in Table 8. A particular SGC may inherit more than one KT at the same time during the operational life of the SGC.

Table 8 – SGC types and key types

KT	SGC type	VendingKey type (see 6.5.2.2.1)	DecoderKey type (see 6.5.2.3.1)
0	Initialization	Not specified	DITK
1	Default	VDDK	DDTK
2	Unique	VUDK	DUTK
3	Common	VCDK	DCTK

See also C.3.2 for Code of practice on managing this data element.

6.1.7 TI: TariffIndex

A 2-digit number associated with a particular tariff that is allocated to a particular customer. The maintenance and the content of the tariff tables are the responsibility of the utility.

Values less than 10 shall be right justified and left padded with 0 (for example 01, 02.. 09).

The TI is also encoded into the DecoderKey, which means that when a customer is moved from one TI to another, then his DecoderKey will also have to change (see 6.5.2.1).

NOTE The encoding of this value when used in the ControlBlock for Decoder Key Generation (see 6.5.3.2) is as two hexadecimal digits, whereas the encoding as used in the Set2ndSectionDecoderKey token (see 6.2.7.3) is as an 8 bit binary number. In these cases a tariff index of 99 decimal is encoded as binary string 10011001 and 0110 0011 respectively.

See also Clause C.10 for Code of practice on managing this data element.

6.1.8 KRN: KeyRevisionNumber

This is a 1-digit number in the range 1 to 9, which ~~is associated with a version of the VendingKey and with the corresponding DecoderKey~~ uniquely identifies a VendingKey within a SupplyGroup. A payment meter's DecoderKey is associated with the SGC and KRN of the VendingKey from which it is derived.

See 6.5.2.5 for a detailed definition of this data element.

6.1.9 KT: KeyType

This is a 1-digit number in the range 0 to 3 associated with a property of the VendingKey and thus also with the corresponding DecoderKey, which is derived from the VendingKey.

See 6.5.2 for a detailed definition of this data element.

6.1.10 KEN: KeyExpiryNumber

A KEN is associated with each VendingKey by the KMS, and defines the time when a VendingKey and any corresponding DecoderKey will expire, after which it becomes invalid for further use, subject to certain concessions.

The KEN corresponds to the most significant 8 bits of the 24-bit TID. Any token identifier whose most significant 8 bits are greater than a given key's KEN cannot be encrypted or decrypted with that key.

See 6.5.2.6 for a detailed definition of this data element.

See also C.3.4 for Code of practice on managing this data element.

6.1.11 DOE: DateOfExpiry

The use of this date is optional and is associated with a validity period for identity related data that gets encoded onto an identity-carrying device. For example: a payment meter ID card or a second record encoded onto the TokenCarrier together with the token data. In some implementations it is found to be useful to let the customer bring back a used token carrier to serve as his decoder identification to the POS when purchasing his next token. (See for example 5.1.4 and 5.2.4.9 of IEC 62055-51:2007).

This date may also be used, for example, in cases where a consumer has been granted a concessionary tariff for a limited period. The date encoded is the last month for which the card is valid.

DOE is in the format YYMM and shall always contain 4 digits.

Where YY or MM is less than 10, it shall be right justified and left padded with 0 (for example 01, 02, 09, etc.).

When the DOE in the IDRecord is not used, then YYMM = 0000.

DOE code values for the year and month are given in Table 9 and Table 10.

Table 9 – DOE codes for the year

YY	Represents
00	2000 or DOE is not used (see also Table 10)
~~01 – 99~~	~~2001 – 2099~~
01 – 78	2001 – 2078

Table 10 – DOE codes for the month

MM	Represents
00	DOE is not used (see also Table 9)
01 – 12	Jan – Dec
13 – 99	Invalid

6.1.12 BDT: BaseDate

The BaseDate is a date and time marker, from which a token identifier (TID) is calculated (see 6.3.5 for using the BaseDate to calculate a TID).

BaseDate is given with respect to Coordinated Universal Time (UTC) time zone.

In order to accommodate the fact that the 24-bit TID will roll over approximately every 31 years, three BaseDate values are defined and are given in Table 11.

Table 11 – BDT representation

Date	BDT representation
01 January 1993, 00:00:00 UTC	93
01 January 2014, 00:00:00 UTC	14
01 January 2035, 00:00:00 UTC	35

6.2 Tokens

6.2.1 Token definition format

The TokenData element in the APDU is a 66-bit binary number comprising of several fields of smaller data elements, in accordance with which various processes are initiated in the MeterApplicationProcess and various bits of information are transferred to the payment meter registers.

The definition format for the tokens in 6.2.2 to 6.2.14 is given in Table 12.

Table 12 – Token definition format

Name of data element	Example: Class, SubClass, RND, TID, Amount, CRC, etc.
Number of bits	Example: 2 bits, 4 bits, 24 bits, 16 bits, etc.
Range of values	Example: 1, 2, 5-15, etc.

6.2.2 Class 0: TransferCredit

Class	SubClass	RND	TID	Amount	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
0	0 = electricity 1 = water 2 = gas ~~Reserved:~~ 3 = time ~~4 = currency~~ ~~5-15 = future assignment~~				
~~NOTE—The SubClass values 3-4 are reserved by the STS Association for applications other than electricity, gas and water, and values 5-15 are reserved for future assignment.~~					

Class	SubClass	S&E	TID	Amount	CRC_C
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
0	4 = electricity currency 5 = water currency 6 = gas currency 7 = time currency 8-15 = future assignment				

Action: Transfer credit to the payment meter to the value as defined in the Amount field (see 6.3.6) and for the service type as defined in the SubClass field.

6.2.3 Class 1: InitiateMeterTest/Display

Class	SubClass	Control	MfrCode	CRC
2 bits	4 bits	36/28 bits	8/16 bits	16 bits
1	0 = STS defined	Bit position control of test/display number for 2 digit manufacturer codes. Use 36 bits.	0 (8 bits)	
1	1 = STS defined	Bit position control of test/display number for 4 digit manufacturer codes. Use 28 bits	0 (16 bits)	
1	2-5 = reserved for future assignment by the STS Association.	Reserved for future assignment by the STS Association.	Reserved for future assignment by the STS Association.	
1	6-10 = proprietary use.	For 4 digit manufacturer codes. If not used, set to zero (28 bits)	0100-9999 (16 bits)	
1	11-15 = proprietary use	For 2 digit manufacturer codes. If not used, set to zero (36 bits)	00-99 (8 bits)	

Action: Initiate the test or display function in the payment meter in accordance with the bit pattern defined in the Control field (see 6.3.8).

A meter having a 2-digit MfrCode value shall support the 36-bit Control field format and may also optionally support the 28-bit Control field format.

A meter having a 4-digit MfrCode value shall support the 28-bit Control field format and may also optionally support the 36-bit Control field format.

6.2.4 Class 2: SetMaximumPowerLimit

Class	SubClass	RND	TID	MPL	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	0				

Action: Load the maximum power limit register in the payment meter with the value as given in the MPL field (see 6.3.9).

6.2.5 Class 2: ClearCredit

Class	SubClass	RND	TID	Register	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	1				

Action: Clear the corresponding credit register as indicated in the Register field (see 6.3.13) in the payment meter to zero.

6.2.6 Class 2: SetTariffRate

Class	SubClass	RND	TID	Rate	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	2				

Action: Load the tariff rate register in the payment meter with the value given in the Rate field (see 6.3.11).

This token is reserved for future definition by the STS Association.

6.2.7 Key change token set for 64-bit DecoderKey transfer

6.2.7.1 General

For 64-bit DecoderKey transfers the decoder shall support a two-token set and optionally a three-token set.

The two-token set shall comprise of the following tokens:

- Set1stSectionDecoderKey;
- Set2ndSectionDecoderKey.

The three-token set shall comprise of the following tokens:

- Set1stSectionDecoderKey token;
- Set2ndSectionDecoderKey token;

- Set3rdSectionDecoderKey token.

6.2.7.2 Class 2: Set1stSectionDecoderKey

Class	SubClass	KENHO	KRN	RO	Res 3KCT	KT	NKHO	CRC
2 bits	4 bits	4 bits	4 bits	1 bit	1 bit	2 bits	32 bits	16 bits
2	3		1-9	0-1	× 0-1	0-3		

Action: Load the DecoderKeyRegister with the 1st half of the new DecoderKey, ~~subject to an authentic loading of a Set2ndSectionDecoderKey token.~~ See 8.9 for the processing of this token.

For decoders that support the three-token set the 3KCT field shall be set to 1 if Set3rdSectionDecoderKey token is included in the set. It shall be set to 0 if Set3rdSectionDecoderKey token is not included in the set.

6.2.7.3 Class 2: Set2ndSectionDecoderKey

Class	SubClass	KENLO	TI	NKLO	CRC
2 bits	4 bits	4 bits	8 bits	32 bits	16 bits
2	4		0-99		

Action: Load the DecoderKeyRegister with the 2nd half of the new DecoderKey, ~~subject to an authentic loading of a Set1stSectionDecoderKey token.~~ See 8.9 for the processing of this token.

6.2.7.4 Class 2: Set3rdSectionDecoderKey

Class	SubClass	SGC	Res_A	CRC
2 bits	4 bits	24 bits	20 bits	16 bits
2	8	0-999999	0	

NOTE The SGC values 1000000 – 16777215 are for future assignment by the STS Association.

The Res_A reserved bits shall be set to 0.

Action: Load the DecoderKeyRegister with the SGC of the new DecoderKey. See 8.9 for the processing of this token.

6.2.8 Key change token set for 128-bit DecoderKey transfer

6.2.8.1 General

For 128-bit DecoderKey transfers the decoder shall support a four-token set.

The four-token set shall comprise of the following tokens:

- Set1stSectionDecoderKey;
- Set2ndSectionDecoderKey;
- Set3rdSectionDecoderKey;
- Set4thSectionDecoderKey.

The DecoderKey = concatenate(NKHO, NKMO2, NKMO1, NKLO).

The SGC = concatenate(SGCHO, SGCLO).

6.2.8.2 Class 2: Set1stSectionDecoderKey

Class	SubClass	KENHO	KRN	RO	Res_B	KT	NKHO	CRC
2 bits	4 bits	4 bits	4 bits	1 bit	1 bit	2 bits	32 bits	16 bits
2	3		1-9	0-1	0	0-3		
The Res_B reserved bit shall be set to 0.								

Action: Transfer the NKHO bits of the new DecoderKey to the decoder. See 8.9 for the processing of this token.

6.2.8.3 Class 2: Set2ndSectionDecoderKey

Class	SubClass	KENLO	TI	NKLO	CRC
2 bits	4 bits	4 bits	8 bits	32 bits	16 bits
2	4		0-99		

Action: Transfer the NKLO bits of the new DecoderKey to the decoder. See 8.9 for the processing of this token.

6.2.8.4 Class 2: Set3rdSectionDecoderKey

Class	SubClass	SGCLO	NKMO2	CRC
2 bits	4 bits	12 bits	32 bits	16 bits
2	8			

Action: Transfer the NKMO2 bits of the new DecoderKey to the decoder. See 8.9 for the processing of this token.

6.2.8.5 Class 2: Set4thSectionDecoderKey

Class	SubClass	SGCHO	NKMO1	CRC
2 bits	4 bits	12 bits	32 bits	16 bits
2	9			

Action: Transfer the NKMO1 bits of the new DecoderKey to the decoder. See 8.9 for the processing of this token.

6.2.9 Class 2: ClearTamperCondition

Class	SubClass	RND	TID	Pad	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	5			0	

Action: Clear the tamper status register in the payment meter and cancel any resultant control processes that may be in progress due to the tamper condition.

6.2.10 Class 2: SetMaximumPhasePowerUnbalanceLimit

Class	SubClass	RND	TID	MPPUL	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	6				

Action: Load the maximum phase unbalance limit register in the payment meter with the value given in the MPPUL field (see 6.3.10). See also 8.12 for more detail on the action of this function in the payment meter.

6.2.11 Class 2: SetWaterMeterFactor

Class	SubClass	RND	TID	WMFactor	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	7				

Action: Load the water meter factor register in the payment meter with the value given in the WMFactor field (see 6.3.12).

This token is reserved by the STS Association for water applications.

6.2.12 Class 2: Reserved for STS use

Class	SubClass	RND	TID	ResData	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	8-10				

Action: Reserved for future definition by the STS Association.

This token range is reserved for future assignment by the STS Association.

6.2.13 Class 2: Reserved for Proprietary use

Class	SubClass	RND	TID	PropData	CRC
2 bits	4 bits	4 bits	24 bits	16 bits	16 bits
2	11-15				

Action: Defined by manufacturer.

This token range is reserved for proprietary definition and use.

This document does not provide protection against collision between manufacturer uses of this token space. Generation and control of these tokens shall therefore always be under the direct management of the relevant manufacturer and shall never be available on vending systems for general use within STS-compliant payment metering systems.

6.2.14 Class 3: Reserved for STS use

Class	SubClass	Res_B
2 bits	4 bits	60 bits
3	0-15	

Action: Reserved for future definition by the STS Association.

This token range is reserved for future assignment by the STS Association.

6.3 Token data elements

6.3.1 Data elements used in tokens

The data elements given in Table 13 are used in tokens in various combinations and are all encoded in binary format.

Table 13 – Data elements used in tokens

Element	Name	Format	Reference
3KCT	TripletKeyChangeTokenFlag (see also 6.2.7.2)	1 bit	
Amount	TransferAmount (see also 6.2.2)	16 bits	6.3.6
Class	TokenClass (see also 6.2.2 to 6.2.14)	2 bits	6.3.2
Control	InitiateMeterTest/DisplayControlField (see also 6.2.3)	36/28 bits	6.3.8
CRC	CyclicRedundancyCodeCheck (see also 6.2.2 to 6.2.13)	16 bits	6.3.7
CRC_C	CyclicRedundancyCheck_C (see also 6.2.2)	16 bits	6.3.22
KENHO	KeyExpiryNumberHighOrder (see also 6.2.7)	4 bits	6.3.18
KENLO	KeyExpiryNumberLowOrder (see also 6.2.7.3)	4 bits	6.3.19
KRN	KeyRevisionNumber (see also 6.2.7)	4 bits	6.1.8
KT	KeyType (see also 6.2.7)	2 bits	6.1.9
MfrCode	ManufacturerCode (see also 6.2.3)	8/16 bits	6.1.2.3.2
MPL	MaximumPowerLimit (see also 6.2.4)	16 bits	6.3.9
MPPUL	MaximumPhasePowerUnbalanceLimit (see also 6.2.10)	16 bits	6.3.10
NKHO	NewKeyHighOrder (see also 6.2.7)	32 bits	6.3.14
NKLO	NewKeyLowOrder (see also 6.2.7.3)	32 bits	6.3.15
NKMO1	NewKeyMiddleOrder1 (see also 6.2.8.5)	32 bits	
NKMO2	NewKeyMiddleOrder2 (see also 6.2.8.4)	32 bits	
Pad	Pad value with 0 (see also 6.2.9)	16 bits	x
PropData	Proprietary data field (see also 6.2.13)	16 bits	x
Rate	[TariffRate] For future definition (see also 6.2.6)	16 bits	6.3.11
Register	RegisterToClear (see also 6.2.5)	16 bits	6.3.13
Res_A	Reserved for future assignment (see also 6.2.7.4)	20 bits	x
Res_B	Reserved for future assignment (see also 6.2.8.2 and 6.2.14)	1 bits	x
ResData	Reserved data field for future assignment (see also 6.2.12)	16 bits	x
RND	RandomNumber (see also 6.2.2 to 6.2.13)	4 bits	6.3.4
RO	RolloverKeyChange (see also 6.2.7)	1 bits	6.3.20
SGC	SupplyGroupCode (see also 6.2.8)	24 bits	6.1.6
SGCHO	SupplyGroupCodeHighOrder	12 bits	
SGCLO	SupplyGroupCodeLowOrder	12 bits	
SubClass	TokenSubClass (see also 6.2.2 to 6.2.14)	4 bits	6.3.3
S&E	SignAndExponent (see also 6.2.2)	4 bits	6.3.21
TI	TariffIndex (see also 6.2.7.3)	8 bits	6.1.7
TID	TokenIdentifier (see also 6.2.2 to 6.2.13)	24 bits	6.3.5.1

Element	Name	Format	Reference
WMFactor	[WaterMeterFactor] Reserved by the STS Association for water application (see also 6.2.11)	16 bits	6.3.12

6.3.2 Class: TokenClass

Tokens are classified into 4 main functional areas as given in Table 14.

Table 14 – Token classes

TokenClass	Function
0	Credit transfer
1	Non-meter-specific management
2	Meter-specific management
3	Reserved for future assignment by the STS Association

Class 0 and Class 2 tokens are encrypted using the DecoderKey, while Class 1 tokens are not encrypted and can thus be used on any STS-compliant payment meter.

6.3.3 SubClass: TokenSubClass

Further sub-classification of the TokenClass is given in Table 15.

Table 15 – Token sub-classes

Token SubClass	Token Class			
	0	1	2	3
0	TransferCredit (electricity)	InitiateMeterTest/Display for 2-digit MfrCode	SetMaximumPowerLimit	Reserved for future assignment by the STS Association
1	TransferCredit (water)	InitiateMeterTest/Display for 4-digit MfrCode	ClearCredit	
2	TransferCredit (gas)	Reserved for future assignment by the STS Association	SetTariffRate Reserved for future assignment by the STS Association	
3	TransferCredit (time) Reserved by STS Association for connection-time applications		Reserved by STS Association for future assignment	Set1stSectionDecoderKey
4	TransferCredit (currency) Reserved by STS Association for currency applications	Set2ndSectionDecoderKey		
5	Reserved by STS Association for future assignment	Reserved for proprietary use for 4-digit MfrCode	ClearTamperCondition	
6			SetMaximumPhasePowerUnbalanceLimit	
7			SetWaterMeterFactor	
8		Reserved by STS Association for water applications		
9			Reserved by STS Association for future assignment	
10		Reserved for proprietary use for 2-digit MfrCode	Reserved for proprietary use	
11				
12				
13				
14				
15				
3	TransferCredit (time)		Set1stSectionDecoderKey	
4	TransferCredit (electricity currency)		Set2ndSectionDecoderKey	
5	TransferCredit (water currency)		ClearTamperCondition	

6	TransferCredit (gas currency)	Reserved for proprietary use for 4-digit MfrCode	SetMaximumPhasePower UnbalanceLimit	
7	TransferCredit (time currency)		SetWaterMeterFactor Reserved by the STS Association for future assignment	
8	Reserved for future assignment by the STS Association		Set3rdSectionDecoderKey	
9			Set4thSectionDecoderKey	
10			Reserved for future assignment by the STS Association	
11		Reserved for proprietary use for 2-digit MfrCode	Reserved for proprietary use	
12				
13				
14				
15				

6.3.4 RND: RandomNumber

The generation of this 4-bit number will be a snapshot of the four least significant bits of at least a millisecond counter. The inclusion of a random number in the data to be transferred enhances the security of the token transfer by providing a probability of 16:1 that no two tokens containing identical data to be transferred will have the same binary pattern. The control of this data element shall be implemented in a secure environment such as a hardware cryptographic module.

6.3.5 TID: TokenIdentifier

6.3.5.1 TID calculation

The TID field is derived from the date and time of issue and indicates the number of minutes elapsed from ~~an STS base date and time~~ the BaseDate associated with the VendingKey. This field is a 24-bit binary representation of the elapsed minutes.

~~In order to accomodate the fact that the TID will roll over every 31 years, three STS base dates are defined. These are:~~

- ~~• 01 January 1993, 00:00:00;~~
- ~~• 01 January 2014, 00:00:00;~~
- ~~• 01 January 2035, 00:00:00.~~

NOTE The definition of BaseDate now references UTC (see 6.1.12), whereas previously it implicitly referenced local time.

For example: with a date and time format of YYYY:MM:DD:hh:mm:ss the ~~STS~~ BaseDate and time of 1993:01:01:00:00:00 corresponds to a TID value of 0.

The calculation of elapsed minutes shall take leap years into account.

The rule used to determine a leap year is:

- the month of February shall have an extra day in all years that are evenly divisible by 4, except for century years (those ending in -00), which receive the extra day only if they are evenly divisible by 400. Thus 1996 was a leap year whereas 1999 was not, and 1600, 2000 and 2400 are leap years but 1700, 1800, 1900 and 2100 are not.

In the binary representation of the TID the leftmost bit represents the most significant bit.

When calculating the TID the “:ss” value shall be truncated from the actual time.

Examples of TID calculated values are given in Table 16.

Table 16 – TID calculation examples

BDT	Date of issue	Time of issue	Elapsed minutes	Resultant 24-bit TID
93	1 January 1993	00:00:00	0	0000 0000 0000 0000 0000 0000
93	1 January 1993	00:01:45	1	0000 0000 0000 0000 0000 0001
93	25 March 1993	13:55:22	120,355	0000 0001 1101 0110 0010 0011
93	25 March 1996	13:55:22	1,698,595	0001 1001 1110 1011 0010 0011
93	1 November 2005	00:01:55	6,749,281	0110 0110 1111 1100 0110 0001
93	1 December 2015	00:01:05	12,051,361	1011 0111 1110 0011 1010 0001
93	24 November 2024	20:15:00	16,777,215	1111 1111 1111 1111 1111 1111
14	1 January 2014	00:00:00	0	0000 0000 0000 0000 0000 0000
14	24 November 2045	20:15:00	16,777,215	1111 1111 1111 1111 1111 1111
35	1 January 2035	00:00:00	0	0000 0000 0000 0000 0000 0000
35	24 November 2066	20:15:00	16,777,215	1111 1111 1111 1111 1111 1111

In order to prevent token re-use when a BaseDate change is performed, certain operational procedures need to be performed. Refer to Clause C.12 for additional information.

6.3.5.2 SpecialReservedTokenIdentifier

The TokenIdentifier corresponding to 00 h 01 min of each day is reserved for special application tokens and may not be used for any other token.

Using the date and time format of YYYY:MM:DD:hh:mm:ss the reserved TID values correspond to xxxx:xx:xx:00:01:xx.

If a token, other than a special application token is to be generated on a time corresponding to this reserved TID, then 1 min shall be added to the TID.

See also Clause C.5 Code of practice for the management of this special reserved TID.

NOTE The use of special application tokens are optional (see Clause C.12), but the rule for how to use the special reserved TID is mandatory.

6.3.5.3 Multiple tokens generated within the same minute

The POS shall ensure that no legitimately purchased token can carry the same TID as that of any other legitimately purchased token for the same payment meter even if more than one token is purchased within the same minute on the same POS.

If multiple tokens need to be generated within the same minute for the same payment meter, then 1 min shall be added to the TID of each successive token in the set. At the end of the token generating process the POS shall revert back to real time again.

This shall apply to any token that implements a TID.

This shall not apply to special application tokens that implement the SpecialReserved TokenIdentifier (see 6.3.5.2).

For example: if 3 credit tokens A, B and C are generated within the same minute at 13h23 and in sequential order A, B and C, then A shall carry the TID time stamp 13h23, B shall carry time stamp 13h24 and C shall carry 13h25.

6.3.6 Amount: TransferAmount

6.3.6.1 General

TransferAmount is the amount of service units or currency units coded into the Amount field of the token and received by the meter.

The associated unit for the TransferAmount is defined in Table 17.

Table 17 – Units of measure for electricity

Transfer type	Units of measure
Electrical energy	watt-hours × 100 (0,1 kWh)
Electrical power	watts
Electrical currency	10 ⁻⁵ base currency

The STS Association also reserves the transfer types given in Table 18 for other applications.

Table 18 – Units of measure for other applications

Transfer type	Units of measure
Water	~~Litres × 100~~ 0,1 cubic metres
Gas	0,1 cubic metres
Time	0,1 minutes
Currency	Under review
Water currency	10 ⁻⁵ base currency
Gas currency	10 ⁻⁵ base currency
Time currency	10 ⁻⁵ base currency
NOTE The STS Association reserves the right to define other future transfer types for other utility services.	

6.3.6.2 Amount for SubClass 0 to 3

The 16 bits of the ~~transfer~~ Amount field are subdivided into two sections, a base-10 exponent of 2 bits and a mantissa of 14 bits. The bits are numbered from right to left, starting at 0. Bit 15 is the most significant bit of the exponent and Bit 13 is the most significant bit of the mantissa. The bit allocations within this field are illustrated in Table 19.

Table 19 – Bit allocations for the ~~Transfer~~ Amount field for SubClass 0 to 3

Position	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Value	e	e	m	m	m	m	m	m	m	m	m	m	m	m	m	m

The mathematical formula for TransferAmount conversion is as follows:

$$t = 10^e \times m, \text{ for } e = 0$$

or

$$t = (10^e \times m) + \sum_{n=1}^e \left(2^{14} \times 10^{(n-1)} \right), \text{ for } e > 0$$

where:

t is the TransferAmount;

e is the base 10 exponent;

m is the mantissa; and

n is an integer in the range 1 to e inclusive.

All TransferAmount conversions shall be rounded up in favour of the customer. The possible TransferAmount ranges and the associated maximum errors that can arise owing to rounding up are shown in Table 20. Examples of TransferAmount values are given in Table 21.

Table 20 – Maximum error due to rounding

Exponent value	TransferAmount range	Maximum error
0	0000000 to 00016383	0,000
1	0016384 to 00180214	~~0,064~~ 0,055 %
2	0180224 to 01818524	0,055 %
3	1818624 to 18201624	0,055 %

Table 21 – Examples of TransferAmount values for credit transfer

Item	Units purchased	Resultant 16-bit ~~transfer~~ Amount field	~~TransferAmount~~ Units converted and received by the meter
1	0,1 kWh	0000 0000 0000 0001	0,1 kWh
2	25,6 kWh	0000 0001 0000 0000	25,6 kWh
3	1638,3 kWh	0011 1111 1111 1111	1638,3 kWh
4	1638,4 kWh	0100 0000 0000 0000	1 638,4 kWh
5	18022,3 kWh	0111 1111 1111 1111	18022,4 kWh
6	18022,4 kWh	1000 0000 0000 0000	18022,4 kWh
7	181862,3 kWh	1011 1111 1111 1111	181862,4 kWh
8	181862,4 kWh	1100 0000 0000 0000	181862,4 kWh
9	1820162,4 kWh	1111 1111 1111 1111	1820162,4 kWh

6.3.6.3 Amount for SubClass 4 to 7

The bit allocation for Amount field is given in Table 22.

Table 22 – Bit allocations for the Amount field for SubClass 4 to 7

Bit position	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bit value	e_1	e_0	m	m	m	m	m	m	m	m	m	m	m	m	m	m

The final value of e is calculated from e_4 , e_3 , e_2 , e_1 and e_0 , obtained from 6.3.21, Table 29 and Table 22 and assigning them bit values as given in Table 23.

Table 23 – Bit allocations for the exponent e

Bit position	4	3	2	1	0
Bit value	e_4	e_3	e_2	e_1	e_0

$$e = (1 \times e_0) + (2 \times e_1) + (4 \times e_2) + (8 \times e_3) + (16 \times e_4)$$

The mathematical formula for the TransferAmount t conversion is as follows:

$$t = 10^e \times m, \text{ for } e = 0$$

or

$$t = (10^e \times m) + \sum_{n=1}^e \left(2^{14} \times 10^{(n-1)} \right), \text{ for } e > 0$$

where:

t is the TransferAmount;

e is the base 10 exponent;

m is the mantissa; and

n is an integer in the range 1 to e inclusive.

The sign of TransferAmount t is obtained from the value of s given in Table 29 where:

t is positive for $s = 0$;

t is negative for $s = 1$.

All TransferAmount conversions shall be rounded up towards positive infinity in favour of the customer (see Table 24 for examples of rounding negative values).

The maximum error due to rounding is 0,055 %. Examples of TransferAmounts and associated errors due to rounding up are shown in Table 25.

Table 24 – Examples of rounding of negative and positive values

Original units to transfer (units of 10^{-5} base currency)	Rounded units transferred (units of 10^{-5} base currency)
–0,99	0
–12,35	–12
–1000,78	–1000
–2314,99	–2314
0,09	1
1000,23	1001
2315,14	2316

Table 25 – Examples of TransferAmounts and rounding errors

Item	Purchase amount (10 ⁻⁵ base currency)	e	m	Transfer amount (10 ⁻⁵ base currency)	Difference	Rounding error
1	2	0	2	2	0	0,000 %
2	16383	0	16383	16383	0	0,000 %
3	16384	1	0	16384	0	0,000 %
4	16385	1	1	16394	9	0,055 %
5	16386	1	1	16394	8	0,049 %
6	16394	1	1	16394	0	0,000 %
7	16395	1	2	16404	9	0,055 %
8	16404	1	2	16404	0	0,000 %
9	16405	1	3	16414	9	0,055 %
10	180214	1	16383	180214	0	0,000 %
11	180215	2	0	180224	9	0,005 %
12	180216	2	0	180224	8	0,004 %
13	1818524	2	16383	1818524	0	0,000 %
14	1818525	3	0	1818624	99	0,005 %

6.3.7 CRC: CyclicRedundancyCodeCheck

The CRC is a checksum field used to verify the integrity of the data transferred for all tokens, except for Class 0 with SubClass 4 to 7, which uses CRC_C (see 6.3.22). The checksum is derived using the following CRC generator polynomial:

$$x^{16} + x^{15} + x^2 + 1$$

The total length of the data transferred via the token is 66 bits. The last 16 bits comprise the CRC checksum that is derived from the preceding 50 bits. These 50 bits are left padded with 6 binary zeros to make 56 bits. Before calculation, the CRC checksum is initialised to FFFF hex (see example in Table 26).

Table 26 – Example of a CRC calculation

Original 50 bits	0 00 4A 2D 90 0F F2 hex
Left padded to make 7 bytes	00 00 4A 2D 90 0F F2 hex
Checksum calculated	0F FA hex

6.3.8 Control: InitiateMeterTest/DisplayControlField

The initiate payment meter test data field is 36/28 bits long and is used to indicate the type of test to be performed. The particular test is selected by setting the relevant bit to a logic ONE. The permissible field values are defined in Table 27.

Table 27 – Permissible control field values

LS Bit No. = 4	Test No	Action	Condition
All bits = 1	0	Do test No. 2 to 5 plus, optionally, any other; inclusion of test No. 2 is mandatory if implemented	Mandatory
1	1	Test supported load switch(es)	Optional
2	2	Test the payment meter information supported display(s) and/or device(s)	Mandatory Optional
3	3	Display cumulative kWh energy usage register totals	Mandatory
4	4	Display the KRN and KT value	Mandatory
5	5	Display the TI value	Mandatory
6	6	Test the token input reader device	Optional
7	7	Display maximum power limit	Optional
8	8	Display tamper status	Optional
9	9	Display active load power consumption	Optional
10	10	Display software version	Optional Mandatory
11	11	Display phase power unbalance limit	Optional
12	12	Display water meter factor (reserved for future definition by the STS Association)	Mandatory for water payment meter Reserved
13	13	Display tariff rate (reserved for future definition by the STS Association)	Mandatory for currency-based payment meter Reserved
14	14	Display the EA value	Mandatory
15	15	Display number of key change tokens supported	Mandatory
16	16	Display the SGC value	Mandatory for 3 or 4 KCT meters
17	17	Display the KEN value	Mandatory
18	18	Display the DRN value	Mandatory
1419-28/36	Reserved	Reserved for future assignment by the STS Association	Reserved
NOTE The cumulative kWh energy register is defined in 5.11.4 of IEC 62055-31:2005. In the context of electricity metering the term "usage" refers to either active energy, reactive energy or apparent energy cumulative totals, depending on the specific metering application. In the context of water, gas or time, the meaning may be interpreted in the context of the particular metering application.			

All payment meters shall support test number 0; if any of the incorporated tests are not supported the payment meter shall perform the subset of tests that are supported. The optional selection of additional incorporated tests is subject to the supply agreement between the supplier and the utility and shall then form a normative part of this document.

~~This option is~~ In the case where a test is optional, the inclusion of this test shall be subject to the supply agreement between the supplier and the utility and shall ~~not~~ then form a normative part of this document.

In the case where more than one test is specified on a single token, the behaviour of the payment meter shall be agreed between the utility and the supplier and shall ~~not~~ then form a normative part of this document.

6.3.9 MPL: MaximumPowerLimit

The maximum power limit field is a 16-bit field that indicates the maximum power that the load may draw, in watts. Calculation of this field is identical to that of the TransferAmount field (see 6.3.6). See also note in 8.6 for functional requirements of the MeterApplication Process.

6.3.10 MPPUL: MaximumPhasePowerUnbalanceLimit

The maximum phase power unbalance limit field is a 16-bit field that indicates the maximum allowable power difference between phase loads, in watts. Calculation of this field is identical to that of the TransferAmount field (see 6.3.6).

6.3.11 Rate: TariffRate

Reserved for future definition by the STS Association.

6.3.12 WMFactor: WaterMeterFactor

Reserved by the STS Association for water application.

6.3.13 Register: RegisterToClear

A unique 16-bit binary value in the range 0 to FFFF hex; to select the particular register that should be cleared with the ClearCredit token. The defined values are given in Table 28.

Table 28 – Selection of register to clear

Value	Action
0	Clear Electricity Credit register
1	Clear Water Credit register
2	Clear Gas Credit register
3	Clear Time Credit register
4	Clear Currency Credit register
4	Clear Electricity Currency Credit register
5	Clear Water Currency Credit register
6	Clear Gas Currency Credit register
7	Clear Time Currency Credit register
5 8 to FFFE hex	Reserved for future assignment by the STS Association
FFFF hex	Clear all Credit registers in the payment meter

6.3.14 NKHO: NewKeyHighOrder

The high order 32 bits of the new DecoderKey that has been generated (see 6.4.4) and which is to be transferred to the payment meter by means of the token.

6.3.15 NKLO: NewKeyLowOrder

The low order 32 bits of the new DecoderKey that has been generated (see 6.4.4) and which is to be transferred to the payment meter by means of the token.

6.3.16 NKMO1: NewKeyMiddleOrder1

The second most significant 32 bits of the 128-bit DecoderKey that has been generated (see 6.4.4) and which is to be transferred to the payment meter by means of a token.

6.3.17 NKMO2: NewKeyMiddleOrder2

The third most significant 32 bits of the 128-bit DecoderKey that has been generated (see 6.4.4) and which is to be transferred to the payment meter by means of a token.