INTERNATIONAL STANDARD

IEC 62055-41

First edition
2007-05

Electricity metering – Payment systems –

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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XD

For price, see current catalogue

CONTENTS

FOREWORD 6
INTRODUCTION 8

1 Scope 10
2 Normative references 10
3 Terms, definitions and abbreviations 11
3.1 Terms and definitions 11
3.2 Abbreviations 12
3.3 Notation and terminology 14
4 Numbering conventions 15
5 Reference model for the standard transfer specification 16
5.1 Generic payment meter functional reference diagram 16
5.2 STS protocol reference model 17
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier 18
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess 19
5.5 MeterFunctionObjects / companion specifications 20
5.6 ISO transaction reference numbers 20
6 POSToTokenCarrierInterface application layer protocol 21
6.1 APDU: ApplicationProtocolDataUnit 21
6.2 Tokens 27
6.3 Token data elements 30
6.4 TCDUGeneration functions 37
6.5 Security functions 43
7 TokenCarriertoMeterInterface application layer protocol 60
7.1 APDU: ApplicationProtocolDataUnit 60
7.2 APDUExtraction functions 63
7.3 Security functions 66
8 MeterApplicationProcess requirements 73
8.1 General requirements 73
8.2 Token acceptance/rejection 73
8.3 Display indicators and markings 74
8.4 TransferCredit tokens 75
8.5 InitiateMeterTest/Display tokens 75
8.6 SetMaximumPowerLimit tokens 75
8.7 ClearCredit tokens 76
8.8 SetTariffRate tokens 76
8.9 Set1stSectionDecoderKey tokens 76
8.10 Set2ndSectionDecoderKey tokens 76
8.11 ClearTamperCondition tokens 77
8.12 SetMaximumPhasePowerUnbalanceLimit tokens 77
8.13 SetWaterMeterFactor 77
8.14 Class 2: Reserved for STS use tokens 77
8.15 Class 2: Reserved for Proprietary use tokens 77
8.16 Class 3: Reserved for STS use tokens 77
9 KMS: KeyManagementSystem generic requirements 77
10 Maintenance of STS entities and related services 78

10.1 General 78
10.2 Operations 80
10.3 Standardisation 82

Annex A (informative) Guidelines for a KeyManagementSystem (KMS) 86
Annex B (informative) Entities and identifiers in an STS-compliant system 89
Annex C (informative) Code of practice for the implementation of STS-compliant systems 92

Bibliography 102

Table 1 – Data elements in the APDU 21
Table 2 – Data elements in the IDRecord 22
Table 3 – Data elements in the MeterPAN 22
Table 4 – Data elements in the IAIN / DRN 23
Table 5 – Token carrier types 24
Table 6 – DKGA codes 24
Table 7 – EA codes 25
Table 8 – SGC types and key types 25
Table 9 – DOE codes for the year 26
Table 10 – DOE codes for the month 27
Table 11 –Token definition format 27
Table 12 – Data elements used in tokens 30
Table 13 – Token classes 31
Table 14 – Token sub-classes 31
Table 15 – TID calculation examples 33
Table 16 – Units of measure for electricity 34
Table 17 – Units of measure for other applications 34
Table 18 – Bit allocation for the TransferAmount 34
Table 19 – Maximum error due to rounding 35
Table 20 – Examples of TransferAmount values 35
Table 21 – Example of a CRC calculation 35
Table 22 – Permissible control field values 36
Table 23 – Selection of register to clear 37
Table 24 – Classification of vending keys 44
Table 25 – Classification of decoder keys 45
Table 26 – Permitted relationships between decoder key types 49
Table 27 – Definition of the PANBlock 51
Table 28 – Data elements in the PANBlock 51
Table 29 – Definition of the CONTROLBlock 52
Table 30 – Data elements in the CONTROLBlock 52
Table 31 – Range of applicable decoder reference numbers 52
Table 32 – List of applicable supply group codes 53

Table 33 – Sample substitution tables 57
Table 34 – Sample permutation table 58
Table 35 – Data elements in the APDU 61
Table 36 – Possible values for the AuthenticationResult 61
Table 37 – Possible values for the ValidationResult 62
Table 38 – Possible values for the TokenResult 62
Table 39 – Values stored in the DKR 67
Table 40 – Sample permutation table 68
Table 41 – Sample substitution tables 69
Table 42 – Entities/services requiring maintenance service 73
Table A.1 – Entities that participate in KMS processes 86
Table A.2 – Processes surrounding the payment meter and DecoderKey 87
Table A.3 – Processes surrounding the CryptographicModule 87
Table A.4 – Processes surrounding the SGC and VendingKey 88
Table B.1 – Typical entities deployed in an STS-compliant system 90
Table B.2 – Identifiers associated with the entities in an STS-compliant system 91
Table C.1 – Data elements associated with a SGC 93
Table C.2 – Data elements associated with the CryptographicModule 94
Table C.3 – Items that should be noted in purchase orders and tenders 97

Figure 1 – Functional block diagram of a generic single-part payment meter 16
Figure 2 – STS modelled as a 2-layer collapsed OSI protocol stack 17
Figure 3 – Dataflow from the POSApplicationProcess to the TokenCarrier 18
Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess 19
Figure 5 – Composition of ISO transaction reference number 20
Figure 6 – Transposition of the 2 Class bits 38
Figure 7 – TCDUGeneration function for Class 0, 1 and 2 tokens 39
Figure 8 – TCDUGeneration function for Set1stSectionDecoderKey token 40
Figure 9 – TCDUGeneration function for Set2ndSectionDecoderKey token 42
Figure 10 – DecoderKey changes – State diagram 48
Figure 11 – DecoderKeyGenerationAlgorithm01 53
Figure 12 – DecoderKeyGenerationAlgorithm02 54
Figure 13 – DecoderKeyGenerationAlgorithm03 55
Figure 14 – STA: EncryptionAlgorithm07 56
Figure 15 – STA encryption substitution process 57
Figure 16 – STA encryption permutation process 58
Figure 17 – STA encryption DecoderKey rotation process 58
Figure 18 – STA encryption worked example for TransferCredit token 59
Figure 19 – DEA: EncryptionAlgorithm09 60
Figure 20 – APDUExtraction function 63
Figure 21 – Extraction of the 2 Class bits 64
Figure 22 – STA DecryptionAlgorithm07 67

Figure 23 – STA decryption permutation process 68
Figure 24 – STA decryption substitution process 69
Figure 25 – STA decryption DecoderKey rotation process 70
Figure 26 – STA decryption worked example for TransferCredit token 70
Figure 27 – DEA DecryptionAlgorithm09 71
Figure A.1 – KeyManagementSystem and interactive relationships between entities 86
Figure B.1 – Entities and identifiers deployed in an STS-compliant system 89

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

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.

The IEC draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the SpecialReservedTokenIdentifier given in 6.3.5.2.

The IEC takes no position concerning the evidence, validity and scope of these patent rights. The holder of these patent rights has assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patents are registered with the IEC. Information may be obtained from:

Address: Actaris Measurement and Systems, P.O. Box 4059,TygerValley 7536, Republic of South Africa

Tel: +27 21 914 3640

Fax: +27 21 914 3630

Website: http://www.actaris.com

Address: Merlin Gerin SA (Pty) Ltd t/a Conlog, P.O. Box 2332, Durban 4000, Republic of South Africa

Tel: +27 31 2681141

Fax: +27 31 2087790

Website: http://www.conlog.co.za

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

This standard cancels and replaces IEC/PAS 62055-41 published in 2003. This first edition constitutes a technical revision.

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

CDV	Report on voting
13/1405/CDV	13/1409/RVC

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

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

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

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

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

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

Part 21: Framework for standardization

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

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

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

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

The Part 4x series specifies application layer protocols and the Part 5x series specifies physical layer protocols.

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

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

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

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

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

Although the main implementation of the STS is in the electricity supply industry, it inherently provides for the management of other utility services like water and gas. Future revisions of the STS may allow for other token carrier technologies like smart cards and memory keys with two-way functionality and to cater for a real-time clock and complex tariffs in the payment meter.

Not all the requirements specified in this standard are compulsory for implementation in a particular system configuration, and, as a guideline, a selection of optional configuration parameters are listed in Clause C.11.

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

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

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 POSToTokenCarrierInterface 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 MeterApplicationProcess in response to tokens received;
- a scheme for dealing with payment meter functionality in the MeterApplicationProcess and associated companion specifications;
- generic requirements for an STS-compliant KeyManagementSystem;
- guidelines for a KeyManagementSystem;
- entities and identifiers used in an STS system;
- a 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.

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

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

2 Normative references

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

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

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

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

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

IEC 62055-52, *Electricity metering – Payment systems – Part 52: Standard transfer specification – Physical layer protocol for a two-way virtual token carrier for direct local connection*[1]

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

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

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

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

---

[1] To be published.