IEC 62055-41

Edition 3.0 2018-03
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 17.220.20; 35.100.70; 91.140.50

ISBN 978-2-8322-5556-8

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

CONTENTS

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 IECEE CB scheme~~

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

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

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

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

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

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

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

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

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

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

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

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

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

1 Scope

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

It specifies:

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEC 62055-41

Edition 3.0 2018-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

FOREWORD

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

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

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

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

Part 21: Framework for standardization

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ELECTRICITY METERING – PAYMENT SYSTEMS –

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

1 Scope

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

It specifies:

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

COMPTAGE DE L'ÉLECTRICITÉ – SYSTÈMES DE PAIEMENT –

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

AVANT-PROPOS

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

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

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

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

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

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

Le texte de cette norme est issu des documents suivants:

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COMPTAGE DE L'ÉLECTRICITÉ – SYSTÈMES DE PAIEMENT –

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

1 Domaine d'application

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

Elle spécifie:

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

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

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

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

2 Références normatives

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

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

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

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

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

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

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

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

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

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

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

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

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