

**Electricity metering –
Payment metering systems –
Part 41:
Standard Transfer Specification**

Withdrawn

P U B L I C L Y A V A I L A B L E S P E C I F I C A T I O N



INTERNATIONAL
ELECTROTECHNICAL
COMMISSION



Reference number
IEC/PAS 62055-41

Withdrawn

**Electricity metering –
Payment metering systems –
Part 41:
Standard Transfer Specification**

Withdrawn

P U B L I C L Y A V A I L A B L E S P E C I F I C A T I O N



INTERNATIONAL
ELECTROTECHNICAL
COMMISSION



Reference number
IEC/PAS 62055-41

CONTENTS

FOREWORD.....	ii
---------------	----

Rationalized User Specification – Electricity sales systems

Part 6: Interface standards

Section 6: Standard transfer specification/Credit dispensing unit – Electricity dispenser – Categories of token and transaction data fields.....	1
Section 7: Standard transfer specification/Credit dispensing unit – Electricity dispenser – Token encoding and data encryption and decryption	17
Section 8: Standard transfer specification/Disposable magnetic token technology – Token encoding format and physical token definition	49
Section 9: Standard transfer specification/Numeric token technology – Token encoding format and physical token definition	63
Part 7: Standard transfer specification/Management of cryptographic keys.....	74
Annex – Standard Transfer Specification – Synopsis.....	103



INTERNATIONAL ELECTROTECHNICAL COMMISSION

ELECTRICITY METERING – PAYMENT METERING SYSTEMS –

Part 41: Standard Transfer Specification

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, 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.
- 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.

A PAS is a technical specification not fulfilling the requirements for a standard, but made available to the public and established in an organization operating under given procedures.

IEC-PAS 62055-41 was submitted by the STS (Standard Transfer Specification) Association and has been processed by IEC technical committee 13: Equipment for electrical energy measurement and load control.

The text of this PAS is based on the following document:

This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document:

Draft PAS	Report on voting
13/1298/PAS	13/1301/RVD

Following publication of this PAS, the technical committee or subcommittee concerned will investigate the possibility of transforming the PAS into an International Standard.

An IEC-PAS licence of copyright and assignment of copyright has been signed by the IEC and the STS association and is recorded at the Central Office.

This PAS shall remain valid for no longer than 3 years starting from 2003-09. The validity may be extended for a single 3-year period, following which it shall be revised to become another type of normative document, or shall be withdrawn.



Withdrawn

ICS 29.240.99; 91.140.50

NRS 009-6-6:2002

Edition 1.1

ISBN 0-626-14112-5

Edition 1: Incorporating Amendment No. 1:2002

Rationalized User Specification

ELECTRICITY SALES SYSTEMS

Part 6: Interface standards

Section 6: Standard transfer specification/Credit dispensing unit — electricity dispenser — Categories of token and transaction data fields

Requirements for applications in the
Electricity Supply
Industry



Gr 8



Standard Transfer Specification

This Rationalized User Specification is
issued by the NRS Project
on behalf of the
User Group given in the foreword
and is not a standard as contemplated in the Standards Act, 1993 (Act 29 of 1993).

Rationalized user specifications allow user organizations to define the performance and quality requirements of relevant equipment.

Rationalized user specifications may, after a certain application period, be introduced as national standards.

Amendments issued since publication

Amdt No.	Date	Text affected
1	May 2002	Notice: Information added on STS compliance. Foreword.
		Clause 2: Normative references updated.
		Clause 3: Note added to clarify abbreviation "ED".
		4.3.2: Reference to NRS 009-4-2 changed to annex A of NRS 009-6-7.

Amendment 1 was compiled to aid understanding of the specification internationally, in preparation for its submission to the IEC, for consideration as an IEC PAS. This consolidated edition 1.1 is technically identical to, and replaces, NRS 009-6-6:1997, which is published by the SABS under ISBN 0-626-11656-2, for which the SABS holds publishing copyright.

Correspondence to be directed to

South African Bureau of Standards
(Electrotechnical Standards)
Private Bag X191
Pretoria 0001

Printed copies obtainable from

South African Bureau of Standards
Private Bag X191
Pretoria 0001

Telephone: (012) 428-7911
Fax: (012) 344-1568
E-mail: sales@sabs.co.za
Website: <http://www.sabs.co.za>

COPYRIGHT RESERVED

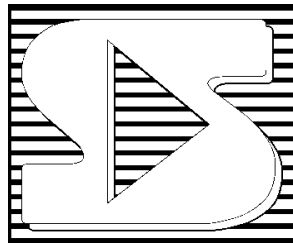
Printed on behalf of the NRS Project in the Republic of South Africa
by the South African Bureau of Standards
1 Dr Lategan Road, Groenkloof, Pretoria



Standard Transfer Specification

NOTICE

Revised February 2003



TM

This section of NRS 009-6 specifies requirements that are part of the standard transfer specification (STS). The intellectual property rights of the STS are owned by the STS Association.¹

The cryptographic algorithms published in this section are those for existing installations and future releases shall make provision for a choice of several state of the art algorithms for implementation according to the strength of the security required in the target installation. It has to be noted that this specification already allows for such alternative algorithms by inference of the data element "Algorithm Code" (see NRS009-6-6 section 4.3.5).

Implementation of an STS compliant system will require access to encryption and decryption tables and the STS encryption keys, which are made available under license conditions through membership of the STS Association. Details of requirements to become a member of the STS Association can be obtained from the contact details given below.

Amdt 1

Suppliers who are to claim that their equipment complies with the STS are required to have the relevant equipment accredited by the STS Association or its agent. Such equipment will be permitted to carry a mark that signifies compliance with the STS.

Application for accreditation of equipment as compliant with the STS can be made to the STS Association:
email@sts.org.za

Amdt 1

Fax number +27(21) 914 3930

Postal address:

PO Box 2332

Durban

4000

South Africa

Further information concerning the STS Association can be obtained from its website:
<http://www.sts.org.za>

Amdt 1

¹ A Section 21 "not for gain" company incorporated in the Republic of South Africa.



This page intentionally left blank



Standard Transfer Specification

Contents

	Page
Foreword.....	2
Introduction	4
Key words	5
1 Scope.....	7
2 Normative references	7
3 Terms, definitions and abbreviated terms.....	8
4 Requirements	8
4.1 General.....	8
4.2 Categories of token.....	8
4.3 Transaction data fields	9



NRS 009-6-6:2002**2****Foreword**

This section of NRS 009-6 has been prepared on behalf of the Electricity Suppliers Liaison Committee (ESLC) and has been approved by it for use by supply authorities in South Africa.

Amendment 1 to this section of NRS 009-6 provides for direct cross-references to NRS 009-4-2, which is not part of the standard transfer specification. The requirements of NRS 009-4-2 that are relevant to this section of NRS 009-6 have been included in an annex to NRS 009-6-7.

Amdt 1

NRS 009 is based on Eskom specification MC114, *Requirements specification for a common vending system for electricity dispensing systems*, and consists of the following parts, under the general title *Electricity sales systems*:

Part 0: Standard transfer specification — Synopsis. (Under consideration.)

Part 1: Glossary and system overview. (Withdrawn, superseded by SABS 1524-0.)

Part 2: Functional and performance requirements.

Section 1: System master stations.

Section 2: Credit dispensing units.

Section 3: Security modules.

Section 4: Standard token translators.

Section 5: Error handling.

Part 3: Database format.

Part 4: National electricity meter cards and associated numbering standards.

Section 1: National electricity meter cards.

Section 2: National electricity meter numbers.

Part 5: Testing of subsystems.

Part 6: Interface standards.

Section 1: Credit dispensing unit — Standard token translator.

Section 2: System master station — main frame.

Section 3: System master station — Credit dispensing unit (previously NRS 009-3).

Section 4: Data transfer by physical media — System master station — Credit dispensing unit.

Section 5: Not allocated

Section 6: Standard transfer specification — Credit dispensing unit — Electricity dispenser — Categories of token and transaction data fields.

Section 7: Standard transfer specification — Credit dispensing unit — Electricity dispenser — Token encoding and data encryption and decryption.

Section 8: Standard transfer specification — Disposable magnetic token technology — Token encoding format and physical token definition.

Section 9: Standard transfer specification — Numeric token technology — Token encoding format and physical token definition.

Part 7: Standard transfer specification — The management of cryptographic keys.

ISBN 0-626-14112-5



Standard Transfer Specification

3

NRS 009-6-6:2002

An amendment to the first edition of this section of NRS 009-6 was submitted by the STS Association in 2002, which was endorsed by a Working Group that comprised the following members:

S J van den Berg (Chairman)	Mangaung Municipality
P A Johnson (Project leader)	NRS Project Management Agency
V Bissett	City of Cape Town
R Devparsad	eThekwini Electricity
J O'Kennedy	Eskom Distribution
V E Rengecas	SABS
M Singh	eThekwini Electricity
D W van Reenen	City Power Johannesburg
J Westenraad	City of Tshwane

The working group acknowledges the contribution of S Leigh, who compiled the standard transfer specification while with Conlog, under a contract to Eskom. The intellectual property rights to the STS have been ceded to the STS Association. See the notice at the front of this section of NRS 009-6.

A Manufacturers' Interest Group (MIG) was consulted on the amendment of this section of NRS 009-6. The MIG comprised the following members:

R Hill	Circuit Breaker Industries
S Leigh	Prism
R Lewis	Tellumat SA
F Pucci	Schneider (t/a Conlog)
A Stoner	Energy Measurements Limited
D Taylor	Actaris Measurements

The Working Group was appointed by the ESLC, which, for the approval of amendment 1, comprised the following members:

R Wienand (Chairman)	eThekwini Metropolitan Council, AMEU
M N Bailey	Distribution Technology, Eskom
A J Claasen	Electrical Engineering Standards, SABS
P Crowdy	Distribution Technology, Eskom
B de Jager	Mangaung Electricity, AMEU
W Dykman	City of Tshwane, AMEU
A H L Fortmann	AMEU
P A Johnson	Technology Standardization, Eskom
J Machinjike	Transmission, Eskom
D M Michie	Nelson Mandela Metropolitan Municipality, AMEU
S V Moodley	City Power Johannesburg (Pty) Ltd
R van der Riet	City of Cape Town, AMEU
J S van Heerden	SABS NETFA
D J van Wyk	uMhlathuze Electricity, AMEU

Recommendations for corrections, additions or deletions should be addressed to the NRS Project Manager, c/o SABS, Private Bag X191, Pretoria, 0001.



Standard Transfer Specification

NRS 009-6-6:2002**4****Introduction**

A variety of proprietary electricity dispensers (EDs) and vending systems have been developed. The proprietary systems are 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 ED and vending equipment have to be operated simultaneously. A standard transfer specification (STS) was developed that would allow for the application of EDs from any manufacturer in an electricity sales (vending) system. The STS is specified in sections 6 to 9 of NRS 009-6 and NRS 009-7.

Amdt 1

The physical device used to transport the information from the vending system to the ED is referred to as a token. The STS specifies the use of two types token. (see NRS 009-6-8 and NRS 009-6-9), namely the disposable magnetic token and the numeric token.

The STS is designed primarily for applications in prepayment electricity sales systems where a secure method for the transfer of purchased electricity units from the credit dispensing unit (CDU) to the ED is required. However, it also caters for the transfer of units of other utility types, for example water or gas.

An overview of the component parts of the STS, as specified in sections 6 to 9 of NRS 009-6, is given in figure 1.

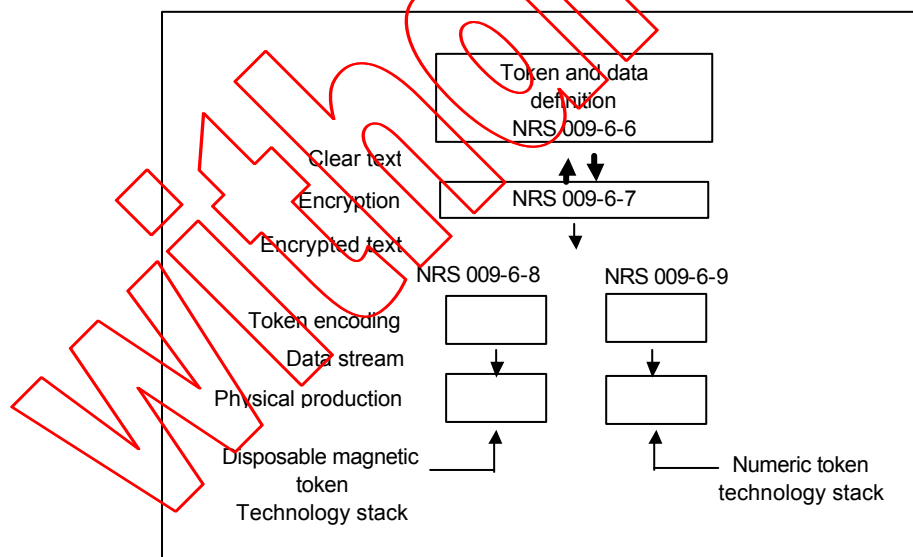


Figure 1 — An overview of the component parts of the STS



Standard Transfer Specification

The STS specifies the following:

- a) categories of tokens (NRS 009-6-6);
- b) transaction data fields (NRS 009-6-6);
- c) encryption algorithm (NRS 009-6-7);
- d) token encoding format and physical token definition for disposable magnetic tokens (NRS 009-6-8);
and
- e) token encoding format and physical token definition for numeric tokens (NRS 009-6-9)

Key words

Electricity sales systems; Payment systems; Prepayment; Standard transfer specification; Electricity dispenser; Token.



Standard Transfer Specification

NRS 009-6-6:2002**6**

This page intentionally left blank



Standard Transfer Specification

SPECIFICATION

Electricity sales systems

Part 6: Interface standards

Section 6: Standard transfer specification/Credit dispensing unit — Electricity dispenser — Categories of token and transaction data fields

Requirements for applications in the Electricity Supply Industry

1 Scope

This section of NRS 009-6, in conjunction with NRS 009-6-7, NRS 009-6-8 and NRS 009-6-9, specifies the standard transfer specification (STS), i.e. the minimum standard for transferring units of credit and information between a common vending system (CVS) and a compliant electricity dispenser (ED).

This section of NRS 009-6 is intended for use by manufacturers of EDs that have to accept tokens that comply with the STS and manufacturers of vending systems that produce STS-compliant tokens.

2 Normative references

The following standard and specifications contain provisions which, through reference in this text, constitute provisions of this section of NRS 009-6. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this section of NRS 009-6 are encouraged to investigate the possibility of applying the most recent editions of the documents listed below. Information on currently valid national and international standards and specifications can be obtained from the South African Bureau of Standards.

NRS 009-6-7:2002, *Electricity sales systems — Part 6: Interface standards — Section 7: Standard transfer specification/Credit dispensing unit — Electricity dispenser — Token encoding and data encryption and decryption.*

Amdt 1

NRS 009-6-8:1997, *Electricity sales systems — Part 6: Interface standards — Section 8: Standard transfer specification/Disposable magnetic token technology — Token encoding format and physical token definition.*

Amdt 1

NRS 009-6-9:1997, *Electricity sales systems — Part 6: Interface standards — Section 9: Standard transfer specification/Numeric token technology — Token encoding format and physical token definition.*

Amdt 1

SABS 1524-0:1997, *Electricity dispensing systems — Part 0: Glossary of terms and system overview.*



Standard Transfer Specification

NRS 009-6-6:2002**8****3 Terms, definitions and abbreviated terms**

For the purposes of this section of NRS 009, the definitions and abbreviations given in SABS 1524-0 apply.

NOTE Throughout this section of NRS 009-6, reference is made to "ED" (electricity dispenser), which is synonymous with "prepayment meter".

Amdt 1

4 Requirements**4.1 General**

An STS-compliant ED shall be capable of reading and interpreting all of the categories of token successfully. Where an optional transaction is not implemented in an ED, the ED shall indicate that the token has been rejected.

4.2 Categories of token

Three categories of token exist, namely:

- a) credit transfer tokens, that are normally used by customers (see 4.2.1);
- b) management tokens that are not ED specific (see 4.2.2); and
- c) management tokens that are ED specific (see 4.2.3).

The use of management tokens is normally restricted to utility personnel.

4.2.1 Credit transfer tokens

The transactions that shall be available using credit transfer tokens are listed in table 1.

Table 1 — Credit transfer token transactions

1	2	3
Description of transaction	STS-compliant ED implementation	ED specific
Transfer electricity units to ED	Mandatory	Yes
Transfer water units to ED	Mandatory if the ED supports water metering	Yes
Transfer gas units to ED	Mandatory if the ED supports gas metering	Yes
Transfer connection time units to ED	Mandatory if the ED supports connection time metering	Yes
Transfer currency units to ED	Mandatory if the ED supports currency metering	Yes

4.2.2 Non-ED-specific management tokens

The transaction that shall be available using non-ED-specific management tokens is a transaction that will initiate an ED test. This transaction is intended for use by installation or maintenance personnel.



Standard Transfer Specification

4.2.3 ED-specific management tokens

The transactions that shall be available using ED-specific management tokens are listed in table 2.

Table 2 — ED-specific management token transactions

1	2	3
Description of transaction	Target user	STS compliant ED implementation
Set maximum power load	Installation or maintenance personnel	Mandatory
Clear ED electricity credit	Installation or maintenance personnel	Mandatory
Clear ED water credit	Installation or maintenance personnel	Mandatory if the ED supports water metering
Clear ED gas credit	Installation or maintenance personnel	Mandatory if the ED supports gas metering
Clear ED connection time credit	Installation or maintenance personnel	Mandatory if the ED supports connection time metering
Clear currency credit	Installation or maintenance personnel	Mandatory if the ED supports currency metering
Set tariff rate	Installation or maintenance personnel	Mandatory if the ED supports currency metering
Set ED key	Installation personnel	Mandatory
Clear tamper condition	Maintenance personnel	Optional
Set phase power unbalance limit	Installation or maintenance personnel	Implementation is mandatory in a poly-phase ED (not applicable in the case of a single-phase ED)
Set water factor	Installation or maintenance personnel	Mandatory if the ED supports water metering

4.3 Transaction data fields

4.3.1 General

The transaction data fields specify the information required to produce the various transactions and the format in which this data will be given. The data fields relevant to each credit transfer transaction are given in table 3. The data fields relevant to the actions effected by non-ED-specific management tokens are given in table 4. The data fields relevant to the transactions effected by ED-specific management tokens are given in table 5.

4.3.2 ED number

The ED number (also known as the meter number) is an 11-digit number, as defined in annex A of NRS 009-6-7.

Amdt 1



NRS 009-6-6:2002**10****4.3.3 Tariff index**

The tariff index is a 2-digit number used in a tariff table to assign the relevant tariff rate to the customer to whom the ED is allocated.

4.3.4 Token technology code

The token technology code is a 2-digit number that is used for the unique identification of the token technology used in an ED.

4.3.5 Algorithm code

The algorithm code is a 2-digit number that is used for the unique identification of the cryptographic algorithm used in the transfer of information via the token.

4.3.6 Supply group code

The supply group code (SGC) is a 6-digit number that is used for the unique identification of the supply group to which the ED belongs.

NOTE The allocation of SGCs is administered nationally in order to avoid their being duplicated. (See annex B of NRS 009-4-1 for information on the use and allocation of SGCs.)

4.3.7 Date of issue

The date of issue is an 8-digit number in the format YYYYMMDD, where YYYY indicates the year of issue, MM indicates the month of issue, and DD indicates the day of issue.

4.3.8 Time of issue

The time of issue is a 6-digit number in the format HHMMSS, where HH indicates the hour of issue (range 00 to 23), MM indicates the minute of issue, and SS indicates the second of issue.

4.3.9 Transfer amount

The transfer amount is an 8-digit number indicating the amount to be transferred, expressed in the appropriate units (see column 9 of table 3).

4.3.10 Maximum power load permitted

The maximum power load permitted in watts, is an 8-digit number.

4.3.11 Phase power unbalance limit

The phase power unbalance limit in watts, is an 8-digit number.

4.3.12 Water factor

The water factor is a 6-digit number used to convert pulses from the water transducer into a form that the ED can use.



Table 3 — Definition of data fields for credit transfer transactions

1	2	3	4	5	6	7	8	9	10
Description of transaction	ED number range	Tariff index range	Token technology code range	Algorithm code range	Supply group code range	Date of issue	Time of issue	Data	ED implementation
Transfer electricity units to ED	0 - 9999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure: 100 watt-hours	The ED shall increase its available credit by the value on the token and store the token identifier to prevent token reuse
Transfer water units to ED	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure: hectolitres	The ED shall increase its available credit by the value on the token and store the token identifier to prevent token reuse
Transfer gas units to ED	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure to be defined	The ED shall increase its available credit by the value on the token and store the token identifier to prevent token reuse
Transfer connection time units to ED	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure: minutes	The ED shall increase its available credit by the value on the token and store the token identifier to prevent token reuse
Transfer currency units to ED	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure to be defined	The ED shall increase its available credit by the value on the token and store the token identifier to prevent token reuse

Table 4 — Definition of data fields for transactions effected by non-ED-specific management tokens

1	2	3	4	5	6	7	8	9	10
Description of management transaction	ED number range	Tariff index range	Token technology code range	Algorithm code range	Supply group code range	Date of issue	Time of issue	Data	ED Implementation
Initiate ED test	N/A	N/A	0 - 99	N/A	N/A	N/A	N/A	Test number 0 - 99	The ED shall react to the test number specified. The test numbers are defined in NRS 009-6-7

NRS 009-6-6:2002

Table 5 — Definition of data fields for transactions effected by ED-specific management tokens

1	2	3	4	5	6	7	8	9	10
Description of management transaction	ED number	Tariff index range	Token technology code range	Algorithm code range	Supply group code range	Date of issue	Time of issue	Data	ED implementation
Set maximum power load	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure: watts	The ED shall update its maximum power load register and store the token identifier to prevent token reuse
Clear credit	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Credit type. Refer to NRS 009-6-7 for actual definitions	The ED shall set the relevant credit balance(s) to zero, and store the token identifier to prevent token reuse
Set tariff rate	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	To be defined	The ED shall update its tariff register and store the token identifier to prevent token reuse
Set dispenser key	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	New supply group code version number 0 - 99. New tariff index 0 - 99	The ED shall overwrite the existing key
Clear tamper condition	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	N/A	The ED shall reset the tamper status register and store the token identifier to prevent token reuse
Set phase power unbalance limit	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 – 18201624 Unit of measure: watts	The ED shall update its maximum phase power unbalance register and store the token identifier to prevent token reuse
Set water factor	0 - 999999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HMMSS	Units 0 - 65535	The ED shall update its water factor register and store the token identifier to prevent token reuse

sabs pta



Standard Transfer Specification

ICS 29.240.99; 35.240.60; 91.140.50

NRS 009-6-7:2002

Edition 2.3

Edition 2: Incorporating
Amendment No. 3:2002

Rationalized User Specification

ELECTRICITY SALES SYSTEMS

Part 6: Interface standards

Section 7: Standard transfer specification/Credit dispensing unit — Electricity dispenser — Token encoding and data encryption and decryption

Requirements for applications in the Electricity Supply
Industry



Gr 10



Standard Transfer Specification

This Rationalized User Specification is
issued by the NRS Project
on behalf of the
User Group given in the foreword
and is not a standard as contemplated in the Standards Act, 1993 (Act 29 of 1993).

Rationalized user specifications allow user organizations to define the performance and quality requirements of relevant equipment.

Rationalized user specifications may, after a certain application period, be introduced as national standards.

Amendments issued since publication

Amdt No.	Date	Text affected
1	May 2001	Subclause 4.2.7:
		a) removed the table of manufacturer codes,
		b) added reference of website for table of manufacturer codes,
		c) added contact details of NRS Projects Manager for list of manufacturer codes,
		d) added reference of specification for meter number.
2	May 2002	Notice: Information added on STS compliance.
		Foreword.
		Clause 2: Normative references updated.
		Clause 3: Note added to clarify abbreviation "ED".
		Subclause 4.2.7 and 4.4. Reference to NRS 009-4-2 changed to reference annex A.
		Annex A added.
3	Feb 2003	Technical corrigendum: Figure 11 and 12, binary value of CRC check sum
		Figure 2, Encryption Algorithm 3 replaced by KMC function and removed accompanying note

Amendment 2 was compiled to aid understanding of the specification internationally, in preparation for its submission to the IEC, for consideration as an IEC PAS. This consolidated edition 2.2 is technically identical to, and replaces, the consolidated edition of NRS 009-6-7:2001, which is published by the SABS under ISBN 0-626-13498-6, for which the SABS holds publishing copyright.

Amendment 3 was compiled to clarify concerns raised by IEC members, pertaining to the IEC/PAS submission and to clarify the apparent conflict in the meaning of Encryption Algorithm 3 as reflected in this document and in the Synopsis document.

Correspondence to be directed to

South African Bureau of Standards
(Electrotechnical Standards)
Private Bag X191
Pretoria 0001

Printed copies obtainable from

South African Bureau of Standards
Private Bag X191
Pretoria 0001

Telephone: (012) 428-7911

Fax: (012) 344-1568



Standard Transfer Specification

E-mail: sales@sabs.co.za
Website: <http://www.sabs.co.za>

COPYRIGHT RESERVED

Printed on behalf of the NRS Project in the Republic of South Africa
by the South African Bureau of Standards
1 Dr Lategan Road, Groenkloof, Pretoria

Withdrawn



Standard Transfer Specification

NOTICE

Revised February 2003



This section of NRS 009-6 specifies requirements that are part of the standard transfer specification (STS). The intellectual property rights of the STS are owned by the STS Association.¹

The cryptographic algorithms published in this section are those for existing installations and future releases shall make provision for a choice of several state of the art algorithms for implementation according to the strength of the security required in the target installation. It has to be noted that this specification already allows for such alternative algorithms by inference of the data element "Algorithm Code" (see NRS009-6-6 section 4.3.5).

Implementation of an STS compliant system will require access to encryption and decryption tables and the STS encryption keys, which are made available under license conditions through membership of the STS Association. Details of requirements to become a member of the STS Association can be obtained from the contact details given below.

Amdt 2

Suppliers who are to claim that their equipment complies with the STS are required to have the relevant equipment accredited by the STS Association or its agent. Such equipment will be permitted to carry a mark that signifies compliance with the STS.

Application for accreditation of equipment as compliant with the STS can be made to the STS Association:
email@sts.org.za

Fax number +27(21) 914 3930

Postal address:
PO Box 2332
Durban
4000
South Africa

Further information concerning the STS Association can be obtained from its website:
<http://www.sts.org.za>

¹ A section 21 "not for gain" company incorporated in the Republic of South Africa.



Standard Transfer Specification

Withdrawn

This page intentionally left blank



Standard Transfer Specification

Contents

	Page
Foreword	2
Introduction	4
Key words	4
1 Scope	5
2 Normative references	5
3 Terms, definitions and abbreviated terms	6
4 Requirements	6
4.1 Bit allocation tables	6
4.2 Field calculations	9
4.3 STS security	16
4.4 Default ED key generation module	17
4.5 Preventing ED-specific token reuse	17
4.6 Encryption algorithm 1	18
4.7 Decryption algorithm 1	20
4.8 Data encryption example	22
4.9 Data decryption example	24
Annex	
A Format of meter numbers used for STS compliant meters	25
Bibliography	27



NRS 009-6-7:2002**2****Foreword**

This section of NRS 009-6 has been adopted by the Electricity Suppliers Liaison Committee (ESLC) and has been approved by it for use by supply authorities in South Africa.

Amendment 2 to this section of NRS 009-6 provides for deletion of direct cross-references to NRS 009-4-2, which is not part of the standard transfer specification. The requirements of NRS 009-4-2 that are relevant to this section of NRS 009-6 have been included in an annex.

NRS 009 is based on Eskom specification MC114, *Requirements specification for a common vending system for electricity dispensing systems*, and consists of the following parts, under the general title *Electricity sales systems*:

Part 0: Standard transfer specification — Synopsis. (Under consideration.)

Part 1: Glossary and system overview. (Withdrawn, superseded by SABS 1524-0.)

Part 2: Functional and performance requirements.

Section 1: System master stations.

Section 2: Credit dispensing units.

Section 3: Security modules.

Section 4: Standard token translators.

Section 5: Error handling.

Part 3: Database format.

Part 4: National electricity meter cards and associated numbering standards.

Section 1: National electricity meter cards

Section 2: National electricity meter numbers.

Part 5: Testing of subsystems.

Part 6: Interface standards.

Section 1: Credit dispensing unit — Standard token translator interface.

Section 2: System master station — Main frame. (Suspended; see annex A of NRS 009-2-1.)

Section 3: System master station — Credit dispensing unit. (Previously NRS 009-3).

Section 4: Data transfer by physical media — System master station — Credit dispensing unit.

Section 5: Not allocated.

Section 6: Standard transfer specification — Credit dispensing unit — Electricity dispenser — Categories of token and transaction data fields.

Section 7: Standard transfer specification — Credit dispensing unit — Electricity dispenser — Token encoding and data encryption and decryption.

Section 8: Standard transfer specification — Disposable magnetic token technology — Token encoding format and physical token definition.

Section 9: Standard transfer specification — Numeric token technology — Token encoding format and physical token definition.

Part 7: Standard transfer specification — The management of cryptographic keys.



Standard Transfer Specification

3**NRS 009-6-7:2002**

An amendment to edition 2.1 of this section of NRS 009-6 was submitted by the STS Association in 2002, which was endorsed by a Working Group that comprised the following members:

S J van den Berg (Chairman)	Mangaung Municipality
P A Johnson (Project leader)	NRS Project Management Agency
V Bissett	City of Cape Town
R Devparsad	eThekweni Electricity
J O'Kennedy	Eskom Distribution
V E Renegacas	SABS
M Singh	eThekweni Electricity
D W van Reenen	City Power Johannesburg
J Westenraad	City of Tshwane

A Manufacturers' Interest Group (MIG) was consulted on the amendment of this section of NRS 009. The MIG comprised the following members:

R Hill	Circuit Breaker Industries
S Leigh	Prism
R Lewis	Tellumat SA
F Pucci	Schneider (t/a Conlog)
A Stoner	Energy Measurements Limited
D Taylor	Actaris Measurements

The working group acknowledges the contribution of S J Leigh, who compiled the standard transfer specification while with Conlog, under a contract to Eskom. The intellectual property rights to the STS have been ceded to the STS Association. See the notice at the front of this section of NRS 009-6.

The Working Group was appointed by the ESLC, which, for the of approval of amendment 2, comprised the following members:

R Wienand(Chairman)	eThekweni Metropolitan Council, AMEU
M N Bailey	Distribution Technology, Eskom
A J Claasen	Electrical Engineering Standards, SABS
P Crowdy	Distribution Technology, Eskom
B de Jager	Mangaung Electricity, AMEU
W Dykman	City of Tshwane, AMEU
A H L Fortmann	AMEU
P A Johnson	Technology Standardization, Eskom
J Machinjike	Transmission, Eskom
D M Michie	Nelson Mandela Metropolitan Municipality, AMEU
S V Moodley	City Power Johannesburg (Pty) Ltd
R van der Riet	City of Cape Town, AMEU
J S van Heerden	SABS NETFA
D J van Wyk	uMhlathuze Electricity, AMEU

Recommendations for corrections, additions or deletions should be addressed to the NRS Project Manager, c/o SABS, Private Bag X191, Pretoria, 0001.

Annex A forms an integral part of this specification.



Standard Transfer Specification

NRS 009-6-7:2002**4****Introduction**

This section of NRS 009-6 is one of a series of specifications that describe the standard transfer specification (STS), whereby transactions can be securely transferred from point of sale equipment to individual electricity dispensers by means of encrypted data on tokens.

The STS is specified in the following parts or sections of NRS 009. Compliance with all the normative (mandatory) requirements of all the following is a requirement for implementation of an STS compliant electricity sales system:

- a) NRS 009-6-6, equivalent to STS Part 1;
- b) NRS 009-6-7, equivalent to STS Parts 2 and 2c;
- c) NRS 009-6-8, equivalent to STS Part 3a;
- d) NRS 009-6-9, equivalent to STS Part 3b; and
- e) NRS 009-7, equivalent to STS Part 2b.

This section of NRS 009-6 describes encryption and decryption processes that are intended primarily for use with tokens in prepayment electricity dispensing systems. However, these tokens can also cater for the transfer of units of other utility types, for example water or gas.

Key words

Electricity sales systems; Payment systems; Prepayment; Standard transfer specification; Electricity dispenser; Token; Token encoding; Data encryption; Data decryption.



Standard Transfer Specification

SPECIFICATION

Electricity sales systems

Part 6: Interface standards

Section 7: Standard transfer specification/Credit dispensing unit — Electricity dispenser — Token encoding and data encryption and decryption

Requirements for applications in the Electricity Supply Industry

1 Scope

This section of NRS 009-6 specifies the formatting of transaction data for encryption, the encryption process and the preparation of the encrypted data for encoding onto the token. It also specifies the decryption process that takes place in the electricity dispenser (ED).

This section of NRS 009-6 is intended for use by manufacturers of EDs that have to accept tokens that comply with the standard transfer specification (STS) and also by manufacturers of vending systems that produce STS-compliant tokens.

2 Normative references

The following standards and specifications contain provisions which, through reference in this text, constitute provisions of this section of NRS 009-6. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this section of NRS 009-6 are encouraged to investigate the possibility of applying the most recent editions of the documents listed below. Information on currently valid national and international standards and specifications can be obtained from the South African Bureau of Standards.

ISO IEC 7812-1:2000, *Identification cards — Identification of issuers — Part 1: Numbering system*.
Amdt 2

SABS 1524-0:1997, *Electricity dispensing systems — Part 0: Glossary of terms and system overview*.

NRS 009-4-2:1993, *Electricity sales systems — Part 4: National electricity meter cards and associated numbering standards — Section 2: National electricity meter numbers*.

NOTE: The requirements of NRS 009-4-2 which are relevant to this section of NRS 009-6 have been included in annex A.

Amdt 2



Standard Transfer Specification

NRS 009-6-7:2002**6****3 Terms, definitions and abbreviated terms**

For the purposes of this section of NRS 009-6, the definitions and abbreviations given in SABS 1524-0 apply.

NOTE Throughout this section of NRS 009-6, reference is made to “ED” (electricity dispenser), which is synonymous with “prepayment meter”.

Amdt 2

4 Requirements**4.1 Bit allocation tables****4.1.1 Credit transfer function bit allocation (Class 00)**

Tokens for credit transfer transactions shall be encoded as set out in table 1. Bits are numbered from right to left starting at 0. A total of 66 bits are used and are numbered from 0 to 65.

Table 1 — Bit allocation for credit transfer functions

1	2	3	4	5	6	7
Function description	Class	Sub-class	Random pattern	Token identifier	Transfer amount	Cyclic redundancy check sum
Electricity credit	00	0000	Length 4 bits Occupies bits 56 to 59 (inclusive) (See 4.2.5)	Length 24 bits Occupies bits 32 to 55 (inclusive) (See 4.2.3)	Length 16 bits Occupies bits 16 to 31 (inclusive) (See 4.2.4)	Length 16 bits Occupies bits 0 to 15 (inclusive) (See 4.2.6)
Water credit	00	0001				
Gas credit	00	0010				
Connection time credit	00	0011				
Currency credit	00	0100				
Reserved for future STS use	00	0101				
	00	0110				
	00	0111				
	00	1000				
	00	1001				
	00	1010				
	00	1011				
	00	1100				
	00	1101				
	00	1110				
	00	1111				
These 64 bits are encrypted						



Standard Transfer Specification

4.1.2 Non-ED-specific management function bit allocation table (Class 01)

Tokens for non-ED-specific management transactions shall be encoded as set out in table 2. Bits are numbered from right to left starting at 0. A total of 66 bits are used and are numbered from 0 to 65.

Table 2 — Bit allocation for non-ED-specific management functions

1	2	3	4	5	6
Function description	Class	Sub-class	Data field	Manufacturer No.	Cyclic redundancy check sum
Initiate ED test	01	0000	Length 36 bits. (See 4.2.8)	0000 0000	Length 16 bits Occupies bits 0 to 15 (inclusive) (See 4.2.6)
Reserved for future STS use	01	0001	Reserved for future STS use	0000 0000	
	01	0010		0000 0000	
	01	0011		0000 0000	
	01	0100		0000 0000	
	01	0101		0000 0000	
	01	0110		0000 0000	
	01	0111		0000 0000	
	01	1000		0000 0000	
	01	1001		0000 0000	
	01	1010		0000 0000	
Reserved for proprietary use (see note)	01	1011	Length 36 bits Occupies bits 24 to 59 (inclusive) (See 4.2.9)	Length 8 bits Occupies bits 16 to 23 (inclusive) (See 4.2.7)	
	01	1100			
	01	1101			
	01	1111			
			These 64 bits are NOT encrypted		
NOTE Functions allocated to these sub-classes will not be supported by a generic vending system. Manufacturers will have to possess the capability to support these functions.					



NRS 009-6-7:2002

8

4.1.3 ED-specific management function bit allocation (Class 10)

Tokens for ED-specific management transactions shall be encoded as set out in table 3. Bits are numbered from right to left starting at 0. A total of 66 bits are used and are numbered from 0 to 65.

Table 3 — Bit allocation to ED-specific management functions

1	2	3	4	5	6	7	
Function description	Class	Sub-class	Random pattern field (see note)	Token identifier field (see note)	Transfer amount field (see note)	Cyclic redundancy check sum	
Set maximum power load	10	0000	See 4.2.5 (4 bits)	See 4.2.3 (24 bits)	See 4.2.10 (16 bits)		
Clear credit	10	0001			See 4.2.11 (16 bits)		
Set tariff rate	10	0010			See 4.2.12 (16 bits)		
Set 1st section ED key	10	0011	See 4.2.17 (4 bits)	4.2.19 (4 bits)	4.2.20 (4 bits)	See 4.2.14 (32 bits)	
Set 2nd section ED key	10	0100	See 4.2.18 (4 bits)	See 4.2.21 (8 bits)	See 4.2.15 (32 bits)	Length 16 bits Occupies bits 0 to 15 (inclusive) (See 4.2.6)	
Clear tamper condition	10	0101	Length 4 bits Occupies bits 56 to 59 (inclusive) (See 4.2.5)	Length 24 bits Occupies bits 32 to 55 (inclusive) (See 4.2.3)	0000 0000 0000 0000		
Set maximum phase power unbalance limit	10	0110			See 4.2.13 (16 bits)		
Set water factor	10	0111			See 4.2.16 (16 bits)		
Reserved for future STS use	10	1000			Length 16 bits Occupies bits 16 to 31 (inclusive)		
	10	1001					
	10	1010					
Reserved for proprietary use NB: These will not be supported by the common vending system	10	1011					
	10	1100					
	10	1101					
	10	1110					
	10	1111					

These 64 bits are encrypted

NOTE The fields in columns 4, 5 and 6 are conventionally named as shown, assuming credit tokens. The actual use of each field and its length is determined by the specific transaction type.



4.2 Field calculations

4.2.1 Token class

The mapping of the token class to a 2-bit binary field is illustrated in table 4.

Table 4 — Allocation of binary patterns to token classes

1	2
Token class	Token class binary pattern
Credit transfer token	00
Non-ED-specific management token	01
ED-specific management token	10
Reserved for future STS use	11

4.2.2 Token subclass

The mapping of the token subclass to a 4-bit binary field is illustrated in table 5.

Table 5 — Allocation of binary patterns to token subclasses

1	2	3	4	5
Token sub-class binary pattern	Class			
	00	01	10	11
0000	Electricity token	Initiate ED test	Set maximum power load	Reserved for future STS use
0001	Water token	Reserved for future STS use	Clear credit	
0010	Gas token		Set tariff rate	
0011	Connection time token		Set 1 st section ED key	
0100	Currency token		Set 2 nd section ED key	
0101	Reserved for future STS use		Clear tamper condition	
0110			Set maximum phase power unbalance limit	
0111			Set water factor	
1000			Reserved for future STS use	
1001				
1010				
1011	Reserved for proprietary use	Reserved for proprietary use		
1100				
1101				
1110				
1111				



NRS 009-6-7:2002**10****4.2.3 Token identifier**

The token identifier field is derived from the date and time of issue and indicates the number of minutes elapsed from a base date and time. The base date and time is 01 January 1993, 00:00:00. The calculation of elapsed minutes shall take leap years into account. This field is a 24-bit binary representation of the elapsed minutes, the leftmost bit being the most significant bit.

Example 1:

Date of issue:	25 March 1993
Time of issue:	13:55:22
Elapsed minutes:	120 355
Resultant 24-bit token ID:	0000 0001 1101 0110 0010 0011

Example 2:

Date of issue:	25 March 1996
Time of issue:	13:55:22
Elapsed minutes:	1 698 595
Resultant 24-bit token ID:	0001 1001 1110 1011 0010 0011

4.2.4 Transfer amount

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. Bit 13 is the most significant bit of the mantissa. The bit allocations within this field are illustrated in figure 1.

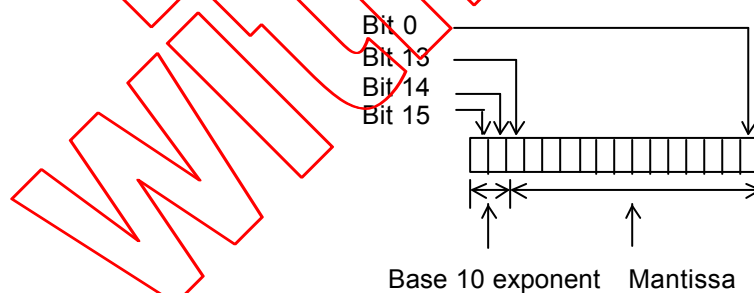


Figure 1 — Allocation of bits in the transfer amount field



11

NRS 009-6-7:2002

The equation for transfer amount conversion is as follows:

$$t = 10^e \cdot m, \text{ for } e = 0; \text{ or}$$

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

where

t is the transfer amount,

e is the exponent,

m is the mantissa, and

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

All transfer amount conversions shall be rounded off in favour of the customer. Table 6 illustrates the possible transfer amount ranges and the associated maximum errors that can arise owing to rounding off.

Table 6 — Maximum errors associated with transfer amount ranges

1	2	3
Exponent value	Transfer amount range	Maximum error
0	0000000 to 00016383	0,000
1	0016384 to 00180214	0,061 %
2	0180224 to 01818524	0,055 %
3	1818624 to 18201624	0,055 %

Examples for credit transfer functions (Class 00)

Example 1:

Units purchased:	26,5 kWh
Resultant 16-bit transfer amount field:	0000 0001 0000 0000

Example 2:

Units purchased:	1 638,4 kWh
Resultant 16-bit transfer amount field:	0100 0000 0000 0000

Example 3:

Units purchased:	181 870,4 kWh
Resultant 16-bit transfer amount field:	1100 0001 0000 0001

