IEC/PAS 62055-41

Edition 1.0
2003-09

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

PUBLICLY AVAILABLE SPECIFICATION

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Reference number
IEC/PAS 62055-41

IEC/PAS 62055-41

Edition 1.0
2003-09

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

PUBLICLY AVAILABLE SPECIFICATION

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Reference number
IEC/PAS 62055-41

CONTENTS

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.

ICS 29.240.99; 91.140.50

ISBN 0-626-14112-5

NRS 009-6-6:2002

Edition 1.1
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

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

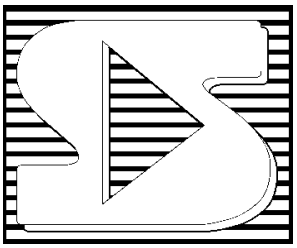
South African Bureau of Standards
Private Bag X191
Pretoria 0001

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

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

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 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

Contents

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

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 of 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.

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.

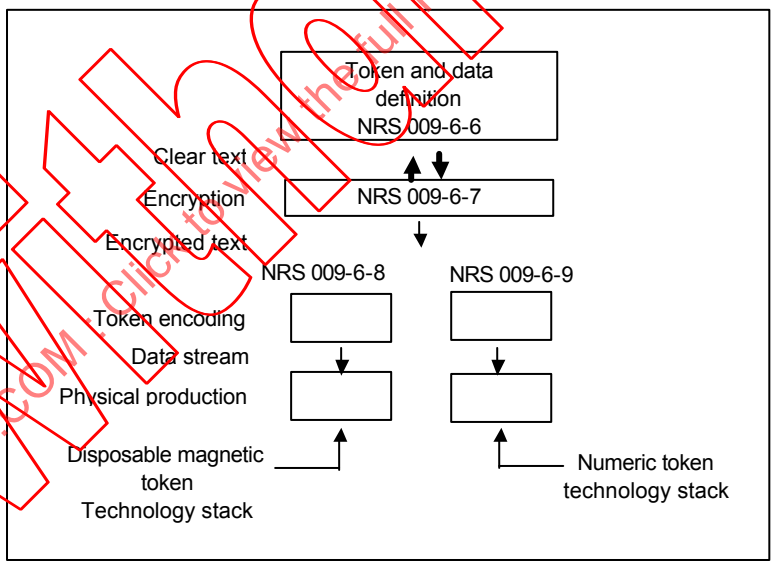


Figure 1 — An overview of the component parts of the STS

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.

This page intentionally left blank

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.*

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.

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

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 techno-logy code range**	**Algorithm code range**	**Supply group code range**	**Date of issue**	**Time of issue**	**Data**	**ED implementation**
Transfer electricity units to ED	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	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	HHMMSS	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 unites to ED	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	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	HHMMSS	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	HHMMSS	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 techno-logy 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

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 techno-logy code range**	**Algorith m code range**	**Supply group code range**	**Date of issue**	**Time of issue**	**Data**	**ED implementation**
Set maximum power load	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	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 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	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 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	To be defined	The ED shall update its tariff register and store the token identifier to prevent token reuse
Set dispenser key	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	New supply group code version number 0 - 99. New tariff index 0 - 99	The ED shall overwrite the existing key
Clear tamper condition	0 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	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 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	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 - 99999999999	0 - 99	0 - 99	0 - 99	0 - 999999	YYYYMMDD	HHMMSS	Units 0 - 65535	The ED shall update its water factor register and store the token identifier to prevent token reuse

sabs pta

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

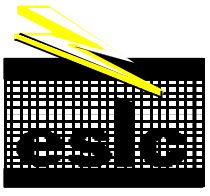
Rationalized User Specification

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

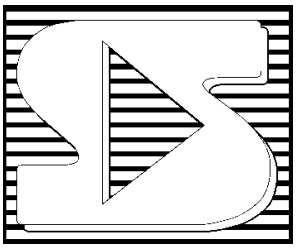
Telephone: (012) 428-7911
Fax: (012) 344-1568

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

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

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.

This page intentionally left blank

Contents

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.

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	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

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)	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.

Annex A forms an integral part of this specification.

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.

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

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			

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

<table>
<tr><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th></tr>
<tr><th>Function description</th><th>Class</th><th>Sub-class</th><th>Data field</th><th>Manufacturer No.</th><th>Cyclic redundancy check sum</th></tr>
<tr><td>Initiate ED test</td><td>01</td><td>0000</td><td>Length 36 bits. (See 4.2.8)</td><td>0000 0000</td><td rowspan="22">Length 16 bits
Occupies
bits 0 to 15
(inclusive)
(See 4.2.6)</td></tr>
<tr><td rowspan="10">Reserved for future STS use</td><td>01</td><td>0001</td><td rowspan="10">Reserved for future STS use</td><td>0000 0000</td></tr>
<tr><td>01</td><td>0010</td><td>0000 0000</td></tr>
<tr><td>01</td><td>0011</td><td>0000 0000</td></tr>
<tr><td>01</td><td>0100</td><td>0000 0000</td></tr>
<tr><td>01</td><td>0101</td><td>0000 0000</td></tr>
<tr><td>01</td><td>0110</td><td>0000 0000</td></tr>
<tr><td>01</td><td>0111</td><td>0000 0000</td></tr>
<tr><td>01</td><td>1000</td><td>0000 0000</td></tr>
<tr><td>01</td><td>1001</td><td>0000 0000</td></tr>
<tr><td>01</td><td>1010</td><td>0000 0000</td></tr>
<tr><td rowspan="5">Reserved for proprietary use (see note)</td><td>01</td><td>1011</td><td rowspan="5">Length 36 bits
Occupies bits 24 to 59
(inclusive)
(See 4.2.9)</td><td rowspan="5">Length 8 bits
Occupies bits
16 to 23
(inclusive)
(See 4.2.7)</td></tr>
<tr><td>01</td><td>1100</td></tr>
<tr><td>01</td><td>1101</td></tr>
<tr><td>01</td><td>1110</td></tr>
<tr><td>01</td><td>1111</td></tr>
<tr><td colspan="6">¬ These 64 bits are NOT encrypted</td></tr>
<tr><td colspan="6">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.</td></tr>
</table>

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

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td>Function description</td><td>Class</td><td>Sub-class</td><td>Random pattern field
(see note)</td><td>Token identifier field
(see note)</td><td>Transfer amount field
(see note)</td><td>Cyclic redundancy check sum</td></tr>
<tr><td>Set maximum power load</td><td>10</td><td>0000</td><td rowspan="3">See 4.2.5
(4 bits)</td><td rowspan="3">See 4.2.3
(24 bits)</td><td>See 4.2.10
(16 bits)</td><td rowspan="3"></td></tr>
<tr><td>Clear credit</td><td>10</td><td>0001</td><td>See 4.2.11
(16 bits)</td></tr>
<tr><td>Set tariff rate</td><td>10</td><td>0010</td><td>See 4.2.12
(16 bits)</td></tr>
<tr><td>Set 1st section ED key</td><td>10</td><td>0011</td><td>See 4.2.17
(4 bits)</td><td>4.2.19
(4 bits)</td><td>4.2.20
(4 bits)</td><td>See 4.2.14
(32 bits)</td></tr>
<tr><td>Set 2nd section ED key</td><td>10</td><td>0100</td><td>See 4.2.18
(4 bits)</td><td>See 4.2.21
(8 bits)</td><td>See 4.2.15
(32 bits)</td><td rowspan="9"></td></tr>
<tr><td>Clear tamper condition</td><td>10</td><td>0101</td><td rowspan="8">Length 4 bits
Occupies
bits 56 to 59
(inclusive)
(See 4.2.5)</td><td rowspan="8">Length 24 bits
Occupies
bits 32 to 55
(inclusive)
(See 4.2.3)</td><td>0000 0000 0000 0000</td></tr>
<tr><td>Set maximum phase power unbalance limit</td><td>10</td><td>0110</td><td>See 4.2.13
(16 bits)</td></tr>
<tr><td>Set water factor</td><td>10</td><td>0111</td><td>See 4.2.16
(16 bits)</td></tr>
<tr><td rowspan="3">Reserved for future STS use</td><td>10</td><td>1000</td><td rowspan="8">Length 16 bits
Occupies
bits 16 to 31
(inclusive)</td></tr>
<tr><td>10</td><td>1001</td></tr>
<tr><td>10</td><td>1010</td></tr>
<tr><td rowspan="5">Reserved for proprietary use
NB: These will not be supported by the common vending system</td><td>10</td><td>1011</td></tr>
<tr><td>10</td><td>1100</td></tr>
<tr><td>10</td><td>1101</td></tr>
<tr><td>10</td><td>1110</td></tr>
<tr><td>10</td><td>1111</td></tr>
<tr><td colspan="7">¬ These 64 bits are encrypted</td></tr>
<tr><td colspan="7">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.</td></tr>
</table>

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

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td rowspan="2">Token sub-class binary pattern</td><td colspan="4">Class</td></tr>
<tr><td>00</td><td>01</td><td>10</td><td>11</td></tr>
<tr><td>0000</td><td>Electricity token</td><td>Initiate ED test</td><td>Set maximum power load</td><td rowspan="16">Reserved for future STS use</td></tr>
<tr><td>0001</td><td>Water token</td><td rowspan="8">Reserved for future STS use</td><td>Clear credit</td></tr>
<tr><td>0010</td><td>Gas token</td><td>Set tariff rate</td></tr>
<tr><td>0011</td><td>Connection time token</td><td>Set 1st section ED key</td></tr>
<tr><td>0100</td><td>Currency token</td><td>Set 2nd section ED key</td></tr>
<tr><td>0101</td><td rowspan="12">Reserved for future STS use</td><td>Clear tamper condition</td></tr>
<tr><td>0110</td><td>Set maximum phase power unbalance limit</td></tr>
<tr><td>0111</td><td>Set water factor</td></tr>
<tr><td>1000</td><td rowspan="4">Reserved for future STS use</td></tr>
<tr><td>1001</td></tr>
<tr><td>1010</td></tr>
<tr><td>1011</td></tr>
<tr><td>1100</td><td rowspan="4">Reserved for proprietary use</td><td rowspan="4">Reserved for proprietary use</td></tr>
<tr><td>1101</td></tr>
<tr><td>1110</td></tr>
<tr><td>1111</td></tr>
</table>

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.

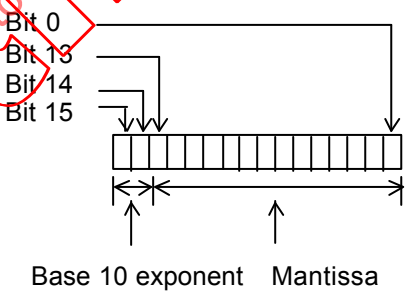


Figure 1 — Allocation of bits in the transfer amount field

The equation for transfer amount conversion is as follows:

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

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

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

4.2.5 Random pattern

The generation of this 4-bit pattern will be a snapshot of the four least significant bits of at least a millisecond counter. The inclusion of a random pattern in the data to be transferred enhances the security of the token transfer by providing a probability that no two tokens containing identical data to be transferred will have the same binary pattern.

4.2.6 Cyclic redundancy check (CRC) check sum

The CRC check sum field is used to verify the correctness of the data transferred. The check sum is derived using the following CRC generator polynomial:

$$X^{16} + X^{15} + X^{2} = 1$$

The total length of the data transferred via the token is 66 bits. The last 16 bits comprise the CRC check sum that is derived from the preceding 50 bits. These 50 bits are left padded with 6 binary zeros to make 56 bits. Before calculation the CRC check sum is initialized to FFFF (hexadecimal). (See example below.)

Example:

Original 50 bits (in hexadecimal)	0 00 4A 2D 90 0F F2
Left padded to make 7 bytes	00 00 4A 2D 90 0F F2
Check sum calculated	0F FA

4.2.7 Manufacturer code

The manufacturer code field is included in the meter number, as specified in NRS 009-4-2. The requirements of NRS 009-4-2 that are relevant to this section of NRS 009-6 are given in annex A.

Amdt 1; amdt 2

4.2.8 Initiate ED test data field

The initiate ED test data field is 36 bits long and is used to indicate the type of test to be performed. The permissible field values are defined in table 8.

Table 8 — Allocation of binary patterns to ED tests

1	2	3
Test No.	**Test description**	**Binary pattern**
0	Incorporates tests 1 to 5 and any optional tests implemented in the ED. This test is mandatory	1111 1111 1111 1111 1111 1111 1111 1111 1111
1	Activates supply disconnect mechanism. This test is mandatory	0000 0000 0000 0000 0000 0000 0000 0000 0001
2	Tests information output devices. This test is mandatory	0000 0000 0000 0000 0000 0000 0000 0000 0010
3	Outputs register totals. This test is mandatory	0000 0000 0000 0000 0000 0000 0000 0000 0100
4	Outputs key revision number. This test is mandatory	0000 0000 0000 0000 0000 0000 0000 0000 1000
5	Outputs tariff index. This test is mandatory	0000 0000 0000 0000 0000 0000 0000 0001 0000
6	Tests token input device. This test is optional	0000 0000 0000 0000 0000 0000 0000 0010 0000
7	Outputs maximum power load. This test is optional	0000 0000 0000 0000 0000 0000 0000 0100 0000
8	Outputs tamper status. This test is optional	0000 0000 0000 0000 0000 0000 0000 1000 0000
9	Outputs power consumption. This test is optional	0000 0000 0000 0000 0000 0000 0001 0000 0000
10	Outputs meter version. This test is optional	0000 0000 0000 0000 0000 0000 0010 0000 0000
11	Outputs phase power unbalance limit. This test is optional	0000 0000 0000 0000 0000 0000 0100 0000 0000
12	Displays water factor. This test is mandatory in a water meter	0000 0000 0000 0000 0000 0000 1000 0000 0000
13	Outputs tariff rate. This test is mandatory in a currency meter	0000 0000 0000 0000 0000 0001 0000 0000 0000

Any optional tests not supported by the ED shall result in the rejection of the optional test token by the ED. All EDs shall support test number 0; if any of the incorporated tests are not supported the ED must perform the subset of tests supported.

4.2.9 Proprietary data field

The proprietary data field is 36 bits long with the left-most bit being the most significant. If this field is not used it shall be set to zero. This data field will not be supported by a common vending system.

4.2.10 Maximum power load units field

The maximum power load units field is a 16-bit field that indicates the maximum power load, in watts. Calculation of this field is identical to that of the transfer amount field (see 4.2.4).

4.2.11 Clear credit field

The clear credit field indicates the type of credit units being cleared. The permitted values for this field are specified in table 9.

Table 9 — Allocation of binary patterns to credit types

1	2
Credit type	**Binary pattern**
Electricity	0000 0000 0000 0000
Water	0000 0000 0000 0001
Gas	0000 0000 0000 0010
Connection time	0000 0000 0000 0011
Currency	0000 0000 0000 0100
Reserved for future STS use	0000 0000 0000 0101 - 1111 1111 1111 1110
Clear all credit registers	1111 1111 1111 1111

4.2.12 Set tariff rate field

The set tariff rate field is a 16-bit field that indicates the tariff rate. The format is still to be defined. This token is intended for future use with currency type units.

4.2.13 Maximum phase power unbalance units field

The maximum phase power unbalance units field is a 16-bit field that indicates the maximum power load, in watts. Calculation of this field is identical to that of the transfer amount field (see 4.2.4).

4.2.14 Set 1st section ED key field

The set 1st section ED key field is 32 bits long and comprises the most significant 4 bytes of the ED key.

4.2.15 Set 2nd section ED key field

The set 2nd section ED key field is 32 bits long and comprises the least significant 4 bytes of the ED key.

4.2.16 Set water factor

The set water factor field is 16 bits long (0-65535) and represents the water factor.

4.2.17 Set 1st section ED key random pattern field

The set 1st section ED key random pattern field is a random 4-bit pattern as defined in 4.2.5.

4.2.18 Set 2nd section ED key random pattern field

The set 2nd section ED key random pattern field is a random 4-bit pattern as defined in 4.2.5.

4.2.19 Key revision number

The key revision number field is a 1-digit (4-bit) number that refers to the revision of the vending key used to derive the meter key.

There must be a maximum of two active vending keys in the credit dispensing unit (CDU), namely the current key and the old key. The **current key** will be used to encrypt all tokens apart from key change tokens; the **old key** will only be used to encrypt key change tokens.

4.2.20 Key change management flags

4.2.20.1 Field definitions

The key change management flags field is a 4-bit field that contains four flags used to denote key change management functions. A flag is set if the value is “1”, and cleared if the value is “0”.

Flag 1	Flag 2	Flag 3	Flag 4

The flags are defined as set out in tables 10a and 10b.

Table 10a — Key change management flags

1	2
Flag	**Description**
1	Roll-over key change
2	Reserved for future use
3	Key type most significant bit
4	Key type least significant bit

Table 10b — Key types

1	2	3
Flag 3	**Flag 4**	**Key type**
0	0	DITK
0	1	DDTK
1	0	DUTK
1	1	DCTK
NOTE Refer to NRS 009-7 for information on key types.		

4.2.20.2 Roll-over key change flag

If the roll-over key change flag is set, the ED shall perform a roll-over key change. This operation is identical to a normal key change, except that the used token identifier stack in the ED is filled with identifiers of value 0 (zero).

4.2.21 Tariff index

The tariff index field is a 2-digit (8-bit) number that refers to the tariff index allocated to the customer. In the event of a newly issued token not being accepted by a customer's ED, this field will enable the supply authority to determine if the token has the correct tariff index.

4.3 STS security

4.3.1 Overview

Figure 2 illustrates the key generation and data encryption processes.

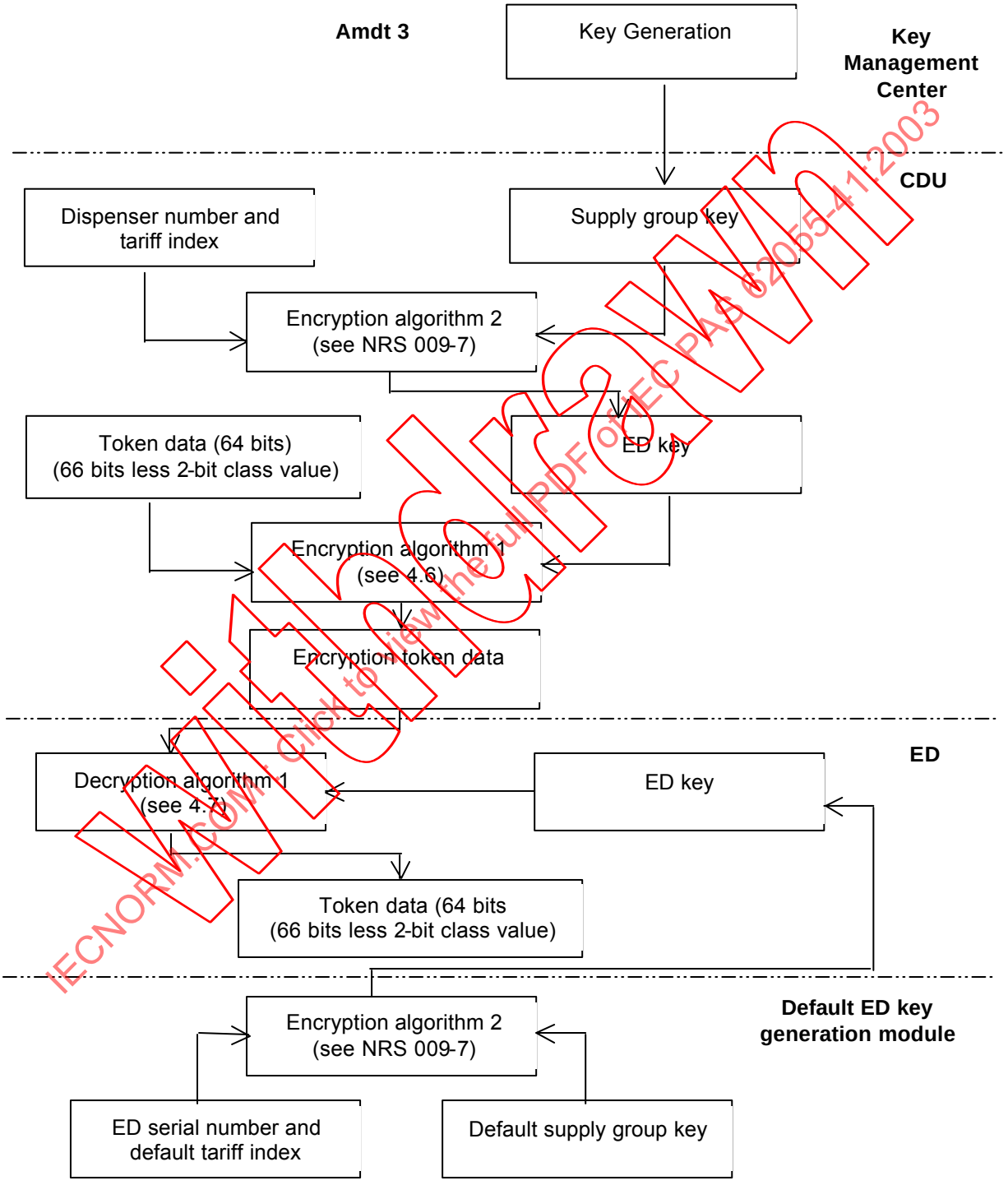


Figure 2 — Key generation and data encryption processes

4.3.2 Default ED key

All EDs shall be shipped from the manufacturer with a default ED key. An ED may not accept a credit transfer token encrypted with a default ED key. This implies that EDs shall then be encoded via the set ED key token before it can accept credit transfer tokens. This can be done at the time of installation.

4.4 Default ED key generation module

The default ED key is generated by a default ED key generation module. This is a device that receives as input the ED's serial number and outputs the default key in ASCII format via an RS232 interface.

The ED's serial number shall be as defined in annex A.

Amdt 2

NOTE Secure management of the derivation and issuing of vending keys is essential for the security of the data encrypted with those keys (see annex D of SABS 1524-0, and NRS 009-7).

4.5 Preventing ED-specific token reuse

The time-based token identifier is used to uniquely identify each ED-specific token. The ED shall store, in the non-volatile memory, at least the last 50 token identifiers received.

Any token identifier received that is already stored shall result in the rejection of the token that contains this identifier.

If a token identifier is received that has a value less than the smallest token identifier stored (in other words, that was issued by a CDU before to the earliest token stored in the ED), the ED shall reject the token containing this identifier.

If a token identifier is received that has a value greater than the smallest token identifier stored (in other words, that is a valid token) and there is no available space in the non-volatile memory to store the received token identifier, the ED shall accept this token, remove the smallest token identifier (in other words, the oldest token) from the non-volatile memory, and replace it with the new token identifier.

If a key change is accepted by the ED, the used token identifier stack shall remain unchanged, unless the roll-over control flag specifies that the stack is cleared.

4.6 Encryption algorithm 1

4.6.1 Description

Encryption algorithm 1 comprises a key alignment process and 16 iterations of a substitution, permutation and key rotation process (see figure 3).

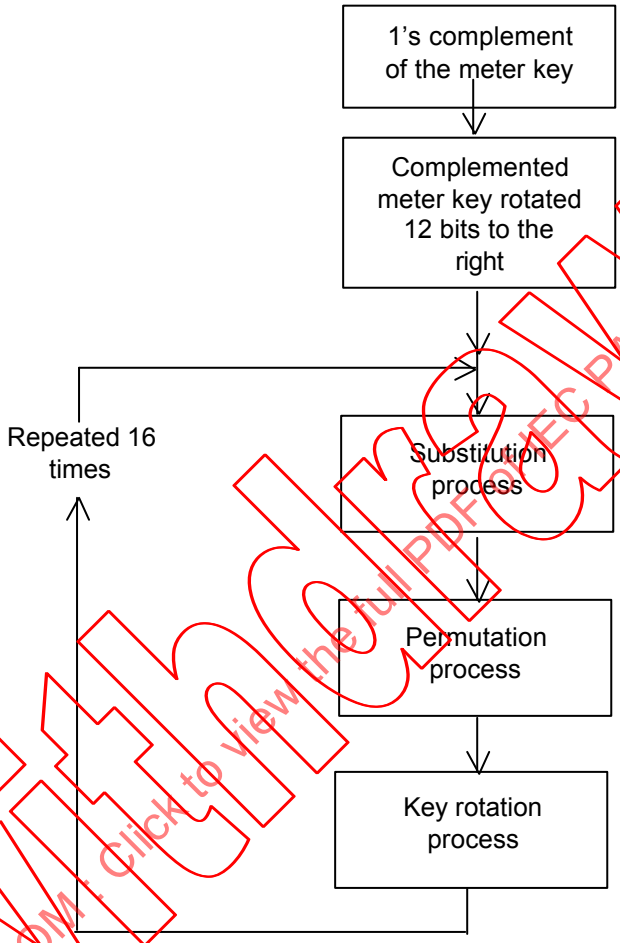


Figure 3 — Illustration of the key generation and data encryption process for algorithm 1

4.6.2 Substitution process

There is a 4-bit substitution process for each of the 16 nibbles in the data stream. The substitution table used is one of two 16-value substitution tables and is dependent on the most significant bit setting of the corresponding nibble in the key. The substitution tables are provided to manufacturers of the systems under licence conditions. The substitution process is illustrated in figure 4 and an example of a substitution table is given in table 11.

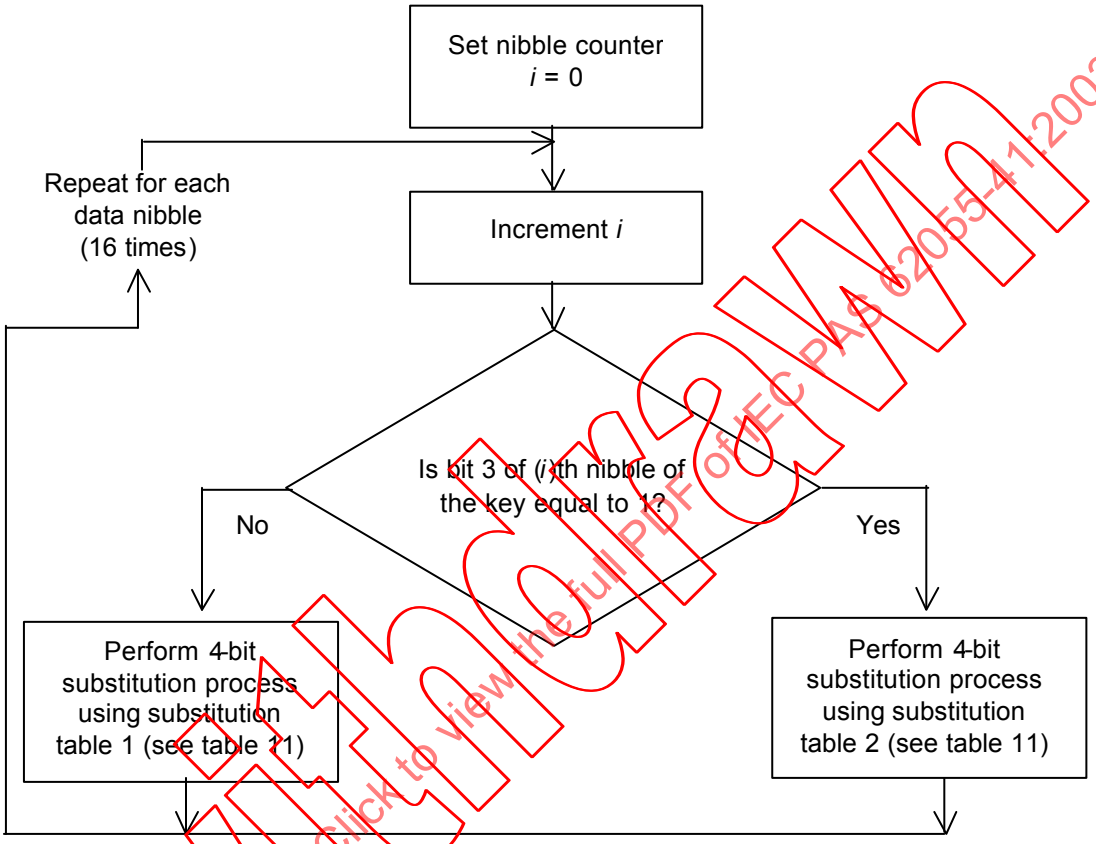


Figure 4 — The substitution process used for encryption

4.6.3 Permutation process

The permutation process is based on a 64-value permutation table and is illustrated in figure 5.

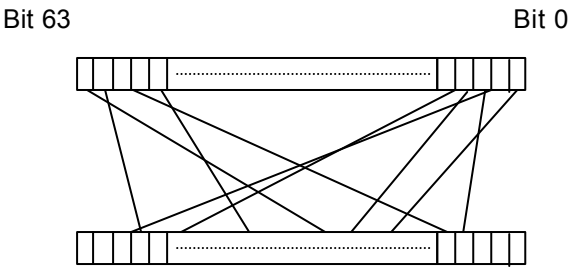


Figure 5 — Illustration of the permutation process used for encryption

The permutation tables are provided to manufacturers of the systems under licence conditions. See the notice prefacing this section of NRS 009-6. (An example of a permutation table is given in table 11.)

4.6.4 Key rotation process

The entire key is rotated 1 bit left, as illustrated in figure 6.

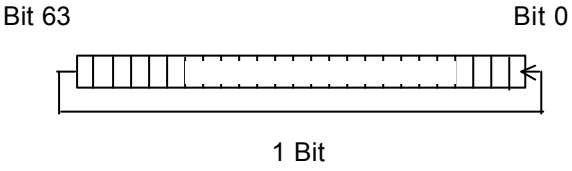


Figure 6 — Illustration of the key rotation process used in encryption

4.7 Decryption algorithm 1

4.7.1 Description

Decryption algorithm 1 comprises 16 iterations of a permutation, substitution and key rotation process. (See figure 7.)

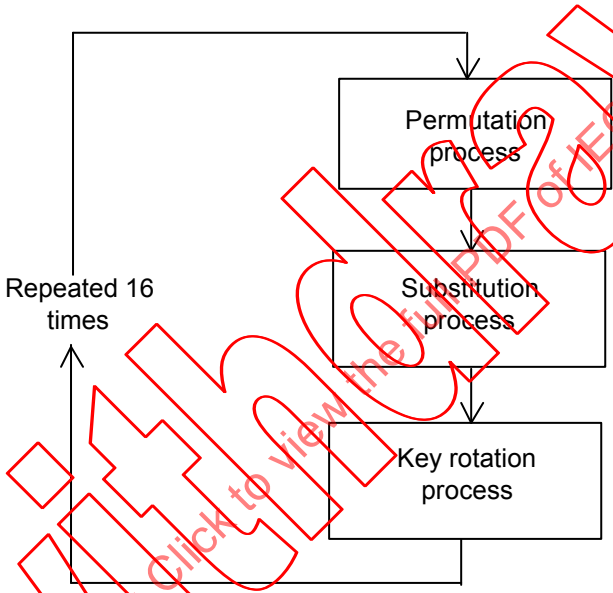


Figure 7 — Illustration of the decryption process for algorithm 1

4.7.2 Permutation process

The permutation process is based on a 64-value permutation table and is illustrated in figure 8.

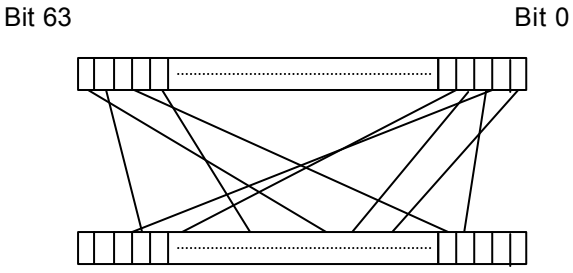


Figure 8 — Illustration of the permutation process used for decryption

The permutation tables are provided to manufacturers of the systems under licence conditions. See the notice prefacing this section of NRS 009-6. (An example of a permutation table used for decryption is given in table 11.)

4.7.3 Substitution process

There is a 4-bit substitution process for each of the 16 nibbles in the data stream. The substitution table used is one of two 16-value substitution tables and is dependent on the least significant bit setting of the corresponding nibble in the key. The substitution tables are provided to manufacturers of the systems under licence conditions. See the notice prefacing this section of NRS 009-6.

The substitution process is illustrated in figure 9, and an example of a substitution table is given in table 12.

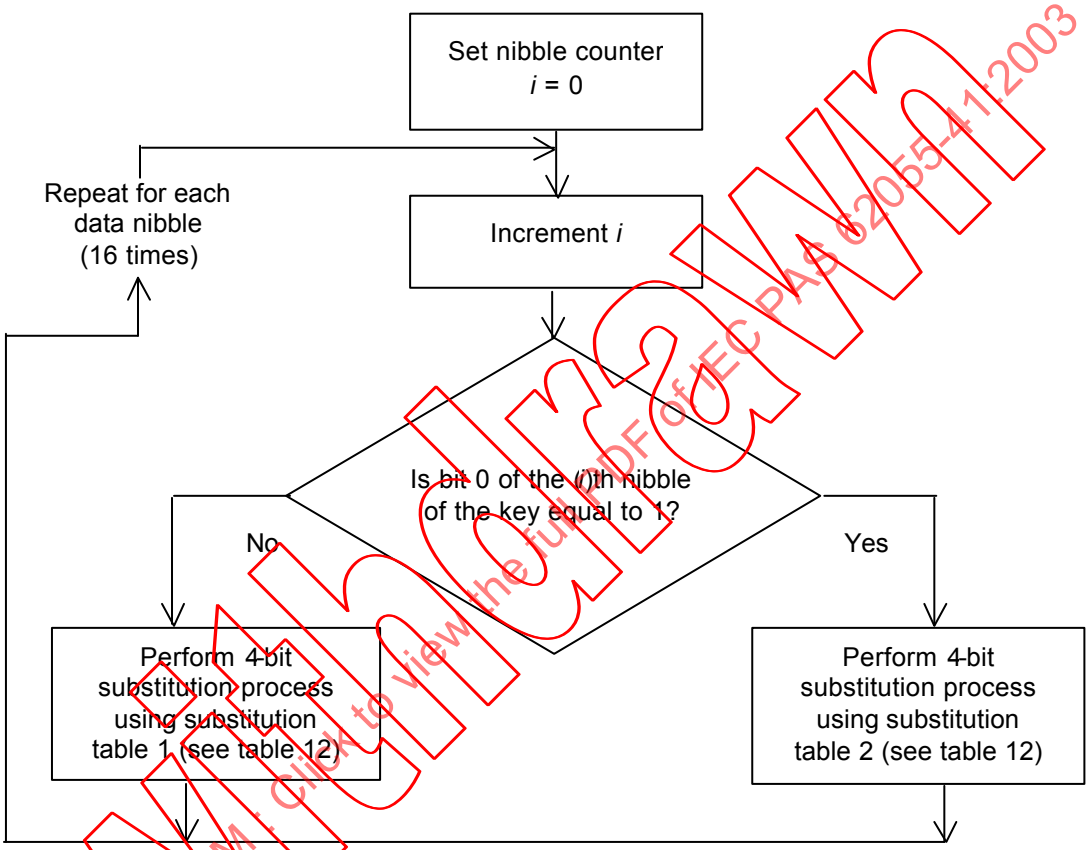


Figure 9 — Illustration of the substitution process used for decryption

4.7.4 Key rotation process

The entire key is rotated 1 bit to the right, as illustrated in figure 10.

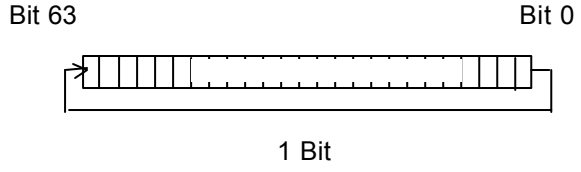


Figure 10 — Illustration of the key rotation process used for decryption

4.8 Data encryption example

4.8.1 Sample tables

For the purpose of the data encryption example given in 4.8.2 the substitution tables and the permutation table in table 11 were used.

Table 11 — Examples of substitution tables and a permutation table used for encryption

1	2
Substitution table 1	12, 10, 8, 4, 3, 15, 0, 2, 14, 1, 5, 13, 6, 9, 7, 11
Substitution table 2	6, 9, 7, 4, 3, 10, 12, 14, 2, 13, 1, 15, 0, 11, 8, 5
Permutation table	29, 27, 34, 9, 16, 62, 55, 2, 40, 49, 38, 25, 33, 61, 30, 23, 1, 41, 21, 57, 42, 15, 5, 58, 19, 53, 22, 17, 48, 28, 24, 39, 3, 60, 36, 14, 11, 52, 54, 12, 31, 51, 10, 26, 0, 45, 37, 43, 44, 6, 59, 4, 7, 35, 56, 50, 13, 18, 32, 47, 46, 63, 20, 8

4.8.2 Worked example of data encryption

An example of data encryption performed in the CDU is shown in figure 11.

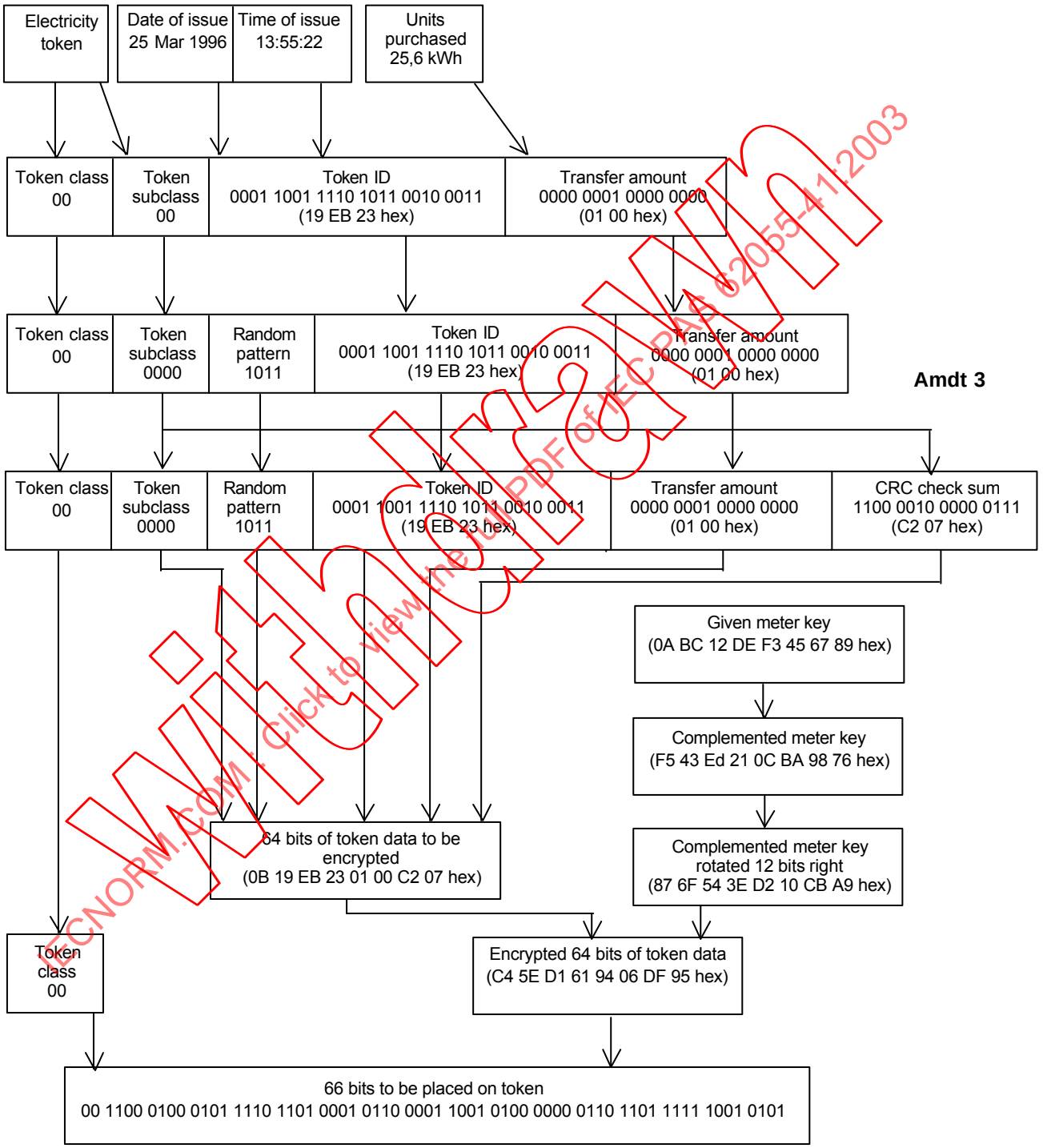


Figure 11 — Example of the encryption process

4.9 Data decryption example

4.9.1 Sample tables

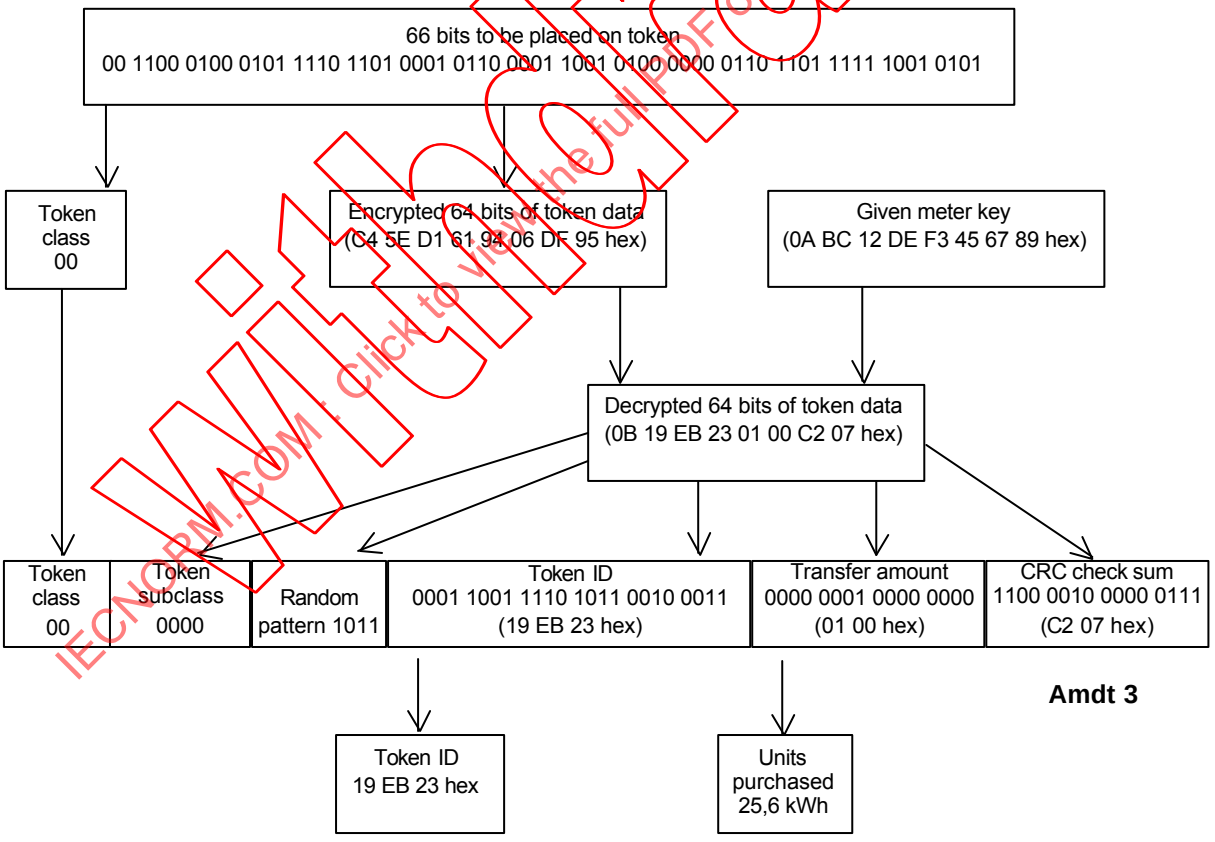
For the purpose of the data decryption example given in 4.9.2 the substitution tables and the permutation table in table 12 were used.

Table 12 — Examples of substitution tables and a permutation table used for decryption

1	2
Substitution table 1	12, 10, 8, 4, 3, 15, 0, 2, 14, 1, 5, 13, 6, 9, 7, 11
Substitution table 2	6, 9, 7, 4, 3, 10, 12, 14, 2, 13, 1, 15, 0, 11, 8, 5
Permutation table	44, 16, 7, 32, 51, 22, 49, 52, 63, 3, 42, 36, 39, 56, 35, 21, 4, 27, 57, 24, 62, 18, 26, 15, 30, 11, 43, 1, 29, 0, 14, 40, 58, 12, 2, 53, 34, 46, 10, 31, 8, 17, 20, 47, 48, 45, 60, 59, 28, 9, 55, 41, 37, 25, 38, 6, 54, 19, 23, 50, 33, 13, 5, 61

4.9.2 Worked example of data decryption

An example of data decryption performed in the ED is shown in figure 12.



Amdt 3

Figure 12 — Example of the decryption process

Annex A
(normative)

Format of meter numbers used for STS compliant meters

NOTE The requirements of this annex are equivalent to requirements extracted from NRS 009-4-2, which is published in South Africa by the SABS.

A.1 Allocation of a meter number

A unique meter number shall be allocated to each STS compliant ED.

A.2 Meter number

The meter number shall contain 11 digits composed in accordance with table A.1 and as explained in 4.2 to 4.4.

Table A.1 — Meter number format

1	2
Manufacturer code (see A.3)	2 digits
Meter serial number (see A.4)	8 digits
Meter number check digit (see A.5)	1 digit
TOTAL	11 digits

A.3 Manufacturer code

The manufacturer code is a 2-digit number that shall be used uniquely to identify the manufacturer of the ED.

The manufacturer codes are allocated and administered by the NRS Project Management Agency (PMA) on behalf of the Electricity Supply Industry (see note). The current list of manufacturer codes can be obtained from the NRS Projects Manager, or viewed on the NRS website: www.nrs.eskom.co.za

NOTE Contact details for the NRS Projects Manager are:

Telephone +27 11 800 3786
Fax +27 11 800 2070
Postal Address:
Technology Standardization
Resources and Strategy Group
PO Box 1091
Johannesburg 2000
South Africa

A.4 Meter serial number

The meter serial number is an 8-digit, unique serial number that can be generated internally by the manufacturer. Each manufacturer is responsible for the uniqueness of the meter serial number with respect to his manufacturer code.

Annex A
(concluded)

A.5 Meter number check digit

The meter number check digit is a single digit used to ensure that the manufacturer code and meter serial number are entered correctly whenever they are entered into the equipment by hand. This is a modulus 10 check digit, calculated using the Luhn formula, as illustrated in annex B of ISO IEC 7812-1. It is calculated on the 10 digits generated through the concatenation of the manufacturer code and the meter serial number.

Amdt 2

Bibliography

ISO 8731-1:1987, *Banking — Approved algorithms for message authentication — Part 1: DEA.*

NRS 009-7:1999, *Electricity sales systems — Part 7: Standard transfer specification — The management of cryptographic keys.*

sabs pta

ICS 29.240.99; 91.140.50

NRS 009-6-8:2003

Second edition

Rationalized User Specification

ELECTRICITY SALES SYSTEMS

Part 6: Interface standards

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

Requirements for applications in the Electricity Supply Industry

esi c

N R S

Gr 7

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
Second edition	January 2003	

Correspondence to be directed to

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

Printed copies obtainable from

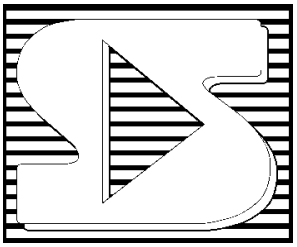
South African Bureau of Standards
Private Bag X191
Pretoria 0001

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

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

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.

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.

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:
E-mail@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

This page intentionally left blank

Contents

Foreword

This second edition of this section of NRS 009-6 has been prepared by the STS Association to

a) delete references to ISO standards that have been either been revised or withdrawn since the publication of the first edition of this section of NRS 009-6;

b) make reference to ISO/IEC 7811-2:2001, *Identification cards - Recording technique - Part 2: Magnetic stripe - Low coercivity*, which replaces the deleted references;

c) amend the relevant requirements clauses to align with the requirements of ISO 7811-2:2001;

d) replace references to NRS 009-4-1 and NRS 009-4-2, with alternative references in the standard transfer specification; and

e) distinguish optional requirements from the mandatory requirements of the standard transfer specification.

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.

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 ¾ System master station ¾ Credit dispensing unit.
Section 5: Not allocated

Section 6: Standard transfer specification — Credit dispensing unit ¾ Electricity dispenser — Categories of token and transaction data fields.
Section 7: Standard transfer specification — Credit dispensing unit ¾ 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.

This second edition of this section of NRS 009-6 was accepted 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, which prepared this second edition of this section of NRS 009-6. See the notice at the front of this section of NRS 009-6.

The Working Group was appointed by the ESLC, which at the time of acceptance of this edition of this section of NRS 009-6, 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
W Dykman	City of Tshwane, AMEU
A H L Fortmann	AMEU
B de Jager	Mangaung Electricity, AMEU
P A Johnson	Technology Standardization, Eskom
R McCurrach	Transmission, Eskom
D M Michie	Nelson Mandela Metropolitan Municipality, AMEU
S V Moodley	City Power Johannesburg (Pty) Ltd
J S van Heerden	SABS NETFA
R van der Riet	City of Cape Town, AMEU
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

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[2] 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 numeric tokens that are intended primarily for use 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; disposable magnetic token.

[2] The term “electricity dispenser” (abbreviated “ED”) is used in this and other parts and sections of NRS 009. It is synonymous with the term “prepayment meter”.

SPECIFICATION

Electricity sales systems

Part 6: Interface standards

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

Requirements for applications in the Electricity Supply Industry

1 Scope

This section of NRS 009-6 details the token encoding format and physical token definition for the disposable magnetic token technology.

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

2 Normative references

The following standard and specification 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 7810:1995, *Identification cards - Physical characteristics.*

ISO 7811-2:2001, *Identification cards - Recording technique - Part 6: Magnetic stripe - Low coercivity.*

NRS 009-6-9:2002, Electricity sales systems - Part 6: Interface standards - Section 9: *Standard transfer specification — Numeric token technology — Token encoding format and physical token definition.*

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

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.

4 Requirements

4.1 Physical token

4.1.1 Token material

The token material shall not be translucent and shall not contain elements that, with time, will degrade the functionality of the magnetic stripe, or affect the reliability with which the data stored on the magnetic stripe on the token can be recovered. This requirement will be deemed to have been met if, after a period of no less than six months, data stored on a sample token held under ambient conditions can be recovered completely.

4.1.3 Token construction

The construction of the token is not specified.

4.1.4 Token characteristics

4.1.4.1 Deformation

The token shall be resistant to damage caused by normal handling, such as being transported on the user's person. The token shall remain functional after first having been deformed within reason and then restored to the extent that it can pass through a slot of 0,4 mm (54,1 mm.)

4.1.4.2 Flammability

Tokens need not be flame resistant.

4.1.4.3 Toxicity

Tokens shall comply with the requirements of 8.1.3 of ISO 7810.

4.1.4.4 Resistance to chemicals

Tokens shall comply with the requirements of 8.1.4 of ISO 7810.

4.1.4.5 Temperature stability

Tokens shall remain structurally reliable and usable at environmental temperatures of between (10 °C and 50 °C.)

NOTE Environmental temperature as defined does not mean card temperature but refers to the environment in which the card is used.

4.1.4.6 Humidity

Tokens shall comply with the requirements of 8.1.5 of ISO 7810.

4.1.4.7 Exposure to light

When exposed to normal household lighting, including fluorescent light or sunlight, for a period of six months, the token shall not degrade to such an extent as to affect the reliability of the magnetic data stored on it.

4.1.4.8 Water resistance

The token shall be water resistant to the extent that if it is immersed in water at 20 °C for 24 h and then dried, the reliability of the magnetic data stored on the token shall not have been affected.

4.1.5 Contamination

The magnetic token material or any other material added to the token shall not contaminate the token reader of the ED in any way.

4.2 Dimensions

The token shall comply with the requirements of 5.1 of ISO 7810 with the exception of 5.1.2, which specifies token thickness.

The token shall be of thickness at least 0,26 mm and shall not exceed 0,34 mm.

NOTE Card-based products have a 1 % expansion characteristic; this is currently under investigation and 4.2 might be amended in the future.

4.3 Location of magnetic stripe area

The magnetic stripe shall be located as specified in ISO/IEC 7811-2 for use of track 3.

4.4 Signal amplitude, encoding technique, encoding specifications

The signal amplitude requirements for magnetic media shall be as specified in ISO/IEC 7811-2.

The encoding technique, the general encoding specifications, and the particular encoding specifications for track 3 shall be as specified in ISO/IEC 7811-2.

4.5 Information contents and formats

The STS token data as set out in table 1 shall be encoded on track 3 of the magnetic stripe.

As an option, additional information may be encoded on track 3. The data can be read at a point of sale from a previously issued token to identify the meter and other relevant attributes. (See Annex A).

Table 1 – STS token data encoded on the token

1	2	3
Data field	**Definition**	**Data field length**
STX	Start sentinel	BCD 11
<data>	20 BCD digits as specified in NRS 009-6-9	20 digits

ETX	End sentinel	BCD 15
LRC	Longitudinal redundancy check	1 digit
TOTAL		23 digits

4.6 Token data erasure

Where so required, it shall be possible for the STS token data to be magnetically erased or rendered unreadable by overwriting the data on the token.

NOTE It is intended that STS compliant meters would erase credit token data after successful transfer of the data to the meter, whereas data on key change tokens would not be erased. (See NRS 009-7 for further information about key change tokens.)

Annex A

(normative)

A.1 Encoding of optional information

Where there is a requirement for an STS token to be encoded with optional information to be read at the point of sale terminal, the information shall be encoded as shown in annex A.

Table A.1 - STS token encoded with additional optional information

1	2	3
Data field	**Definition**	**Data field length**
STX	Start sentinel	BCD 11
<data>	20 BCD digits as specified in NRS 009-6-9	20 digits
ETX	End sentinel	BCD 15
LRC	Longitudinal redundancy check	1 digit
<space data>	33 BCD zeroes	33 digits
STX	Start sentinel	BCD 11
ISO BIN (PAN)	See A.1	6 digits
Meter number	As defined in NRS 009-6-7	11 digits
LRC	Longitudinal redundancy check	1 digit
SEPARATOR	Field separator	BCD 13
Expiry date	See NOTE	4 digits or BCD 13
SEPARATOR	Field separator	BCD 13
Token technology code	See A.2	2 digits
Algorithm code	See A.3	2 digits
Supply group code	As defined in NRS 009-6-6	6 digits
Tariff index	As defined in NRS 009-6-6	2 digits
ETX	End sentinel	BCD 15
LRC	Longitudinal redundancy check	1 digit
TOTAL		95/92 digits
NOTE The expiry date will be used, for example, in cases where a customer has been granted a concessionary tariff for a limited period. The date encoded is the last month of the period, in the form YYMM, where YY represents the year (00 to 78 for years 2000 to 2078), and MM represents the month (01 to 12). Where this date is not required it is replaced by the separator character BCD 13.		

A.2 Data entities used in STS tokens

A.2.1 ISO BIN

The ISO BIN is a six-digit number that may be allocated by ISO to uniquely identify the category of business transaction in a country. The ISO BIN allocated for electricity sales transactions in South Africa is 600727.

A.2.2 Token technology code

The token technology code is a 2-digit number that shall be used uniquely to identify the token technology used in an electricity dispenser. The token technology codes allocated for STS tokens are as shown in table A.2 (NOTE 1)

Table A.2 - STS Token technology codes

1	2
Token technology type	**Token technology code** (See NOTE 3)
STS disposable magnetic token	01
STS numeric token	02

A.2.3 Algorithm code

The algorithm code is a 2-digit number that shall be used uniquely to identify the encryption algorithm used for transactions. The algorithm code allocated to the STS algorithm as specified in NRS 009-6-7 is **07**.(NOTE 1)

NOTE 1 Where STS prepayment systems are required to support vending to proprietary prepayment meters, the relevant token technology codes and algorithm codes will be used. The token technology codes and algorithm codes are allocated and administered by the NRS Project Management Agency (PMA) on behalf of the Electricity Supply Industry. The current list of token technology codes and algorithm codes can be obtained from the NRS Projects Manager (see NOTE 2), or viewed on the NRS website: www.nrs.eskom.co.za.

NOTE 2 Contact details for the NRS Projects Manager are:

Telephone +27 11 800 3786
Fax +27 11 800 2070
Postal Address:
Technology Standardization
Resources and Strategy Group
PO Box 1091
Johannesburg 2000

NOTE 3 The token technology code defines the particular type of token carrier. In the case of numeric tokens, the same token carrier can be used for both STS numeric tokens and proprietary numeric tokens.

sabs pta

ICS 29.240.99; 91.140.50

ISBN 0-626-14118-4

NRS 009-6-9:1997

First edition 1997, reconfirmed 2002

Rationalized User Specification

ELECTRICITY SALES SYSTEMS

Part 6: Interface standards

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

Requirements for applications in the Electricity Supply Industry

esi

N R S

Gr 7

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
Reconfirmed	May 2002	Notice, foreword and introduction. No technical changes.

Correspondence to be directed to

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

Printed copies obtainable from

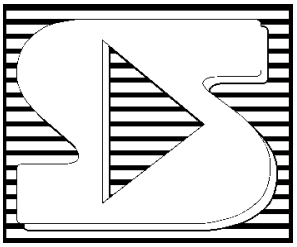
South African Bureau of Standards
Private Bag X191
Pretoria 0001

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

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

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.

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
E-mail@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

This page intentionally left blank

Contents

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.

NRS 009-6 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 ¾ System master station ¾ Credit dispensing unit.
Section 5: Not allocated
Section 6: Standard transfer specification — Credit dispensing unit ¾ Electricity dispenser — Categories of token and transaction data fields.
Section 7: Standard transfer specification — Credit dispensing unit ¾ 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 0-626-14118-4

This first edition of this section of NRS 009-6 was reconfirmed 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 reconfirmation of this edition 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 at the time of reconfirmation of this edition of this section of NRS 009-6, 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
W Dykman	City of Tshwane, AMEU
A H L Fortmann	AMEU
B de Jager	Mangaung Electricity, 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
J S van Heerden	SABS NETFA
R van der Riet	City of Cape Town, AMEU
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

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[2] 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 numeric tokens that are intended primarily for use 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; Numeric token.

[2] The term “electricity dispenser” (abbreviated “ED”) is used in this and other parts and sections of NRS 009. It is synonymous with the term “prepayment meter”.

SPECIFICATION

Electricity sales systems

Part 6: Interface standards

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

Requirements for applications in the Electricity Supply Industry

1 Scope

This section of NRS 009-6 details the token encoding format and physical token definition for the numeric token technology.

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

2 Normative references

The following standard and specification 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.*

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

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.

4 Requirements

4.1 Token encoding format

4.1.1 Introduction

Subclause 4.1 describes the data format for token production as required by the numeric token type.

4.1.2 Binary format

Token data shall be encrypted as specified in NRS 009-6-7. The encrypted 64-bit number has its least significant bit in bit position 0 and its most significant bit in bit position 63 (see figure 1). The encrypted 64-bit binary number string is modified to include the unencrypted token class (see notes 1 and 2). The 2-bit token class is inserted to occupy bit positions 28 and 27. The original values of bit positions 28 and 27 are **relocated** to bit positions 65 and 64. The most significant bit of the token class occupies bit position 28. The most significant bit of the 64-bit encrypted number occupies bit position 63 (see figure 1).

NOTES

1 The token classes are defined in NRS 009-6-7.

2 Because the token class is not encrypted, a consistent pattern could be introduced by including it at the beginning after the binary digit string, which would negate some of the security aspects of the encryption methodology. The token class is therefore inserted into the body of the binary digit string.

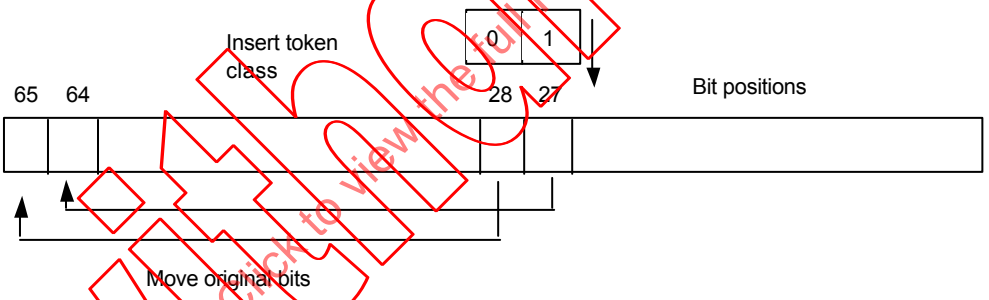


Figure 1

Example 1 — Insertion of the token class

The 64-bit binary number expressed in bytes. (Bits 27 and 28 highlighted in bold.)

0110 0101 0100 0011 0010 0001 0000 1001 100**0** **0**111 0110 0101 0100 0011 0010 0001

Repeat bits 28 and 27 in bit positions 65 and 64, creating a 66-bit number.

00 0110 0101 0100 0011 0010 0001 0000 1001 1000 0111 0110 0101 0100 0011 0010 0001

Replace bits 28 and 27 with the token class

00 0110 0101 0100 0011 0010 0001 0000 1001 100**0** **1**111 0110 0101 0100 0011 0010 0001

4.1.3 Decimal format

The 66-bit binary number shall be presented as a decimal number. This decimal number will be 20 digits long. The decimal number shall represent the binary number in such a way that bit position 0 is the least significant bit.

Example 2 — The conversion from a 66-bit binary number, presented as a binary and a hexadecimal number, to a 20-digit decimal number

Binary number	**11**0110**0101**0100**0011**0010**0001**0000**1001**1000**0111**0110**0101**1010**1011**1100**1101**
Hexadecimal number	3654321098765ABCD
Decimal number	62636944367208999885

4.2 Physical token definition

4.2.1 Introduction

Subclause 4.2 specifies the physical attributes of the token and describes the token production process.

4.2.2 Number presentation

When printed, the 20-digit numeric token number shall be presented on one line, so formatted that the digits are grouped into five groups of four digits with spaces between groups.

Example 3 — The 20-digit numeric token

1234 5678 1234 5678 1234

NOTE The medium for carrying the numeric token is not specified. Typically, it is intended that the digits be printed legibly and indelibly using industry standard receipting printers such as those used in cash registers. However, in principle, the numeric token could also be transferred verbally, for example by telephone.

sabs pta

ICS 91.140.50

ISBN 0-626-12165-5

NRS 009-7:1999

First edition

Rationalized User Specification

ELECTRICITY SALES SYSTEMS

Part 7: Standard transfer specification/Management of cryptographic keys

Preferred requirements for applications in the Electricity Supply Industry

NRS 009-7:1999

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

Correspondence to be directed to

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

Printed copies obtainable from

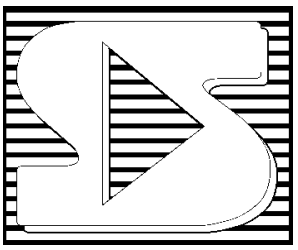
South African Bureau of Standards
Private Bag X191
Pretoria 0001

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

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

NOTICE

Revised February 2003



™

This part of NRS 009 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.

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:
P.O. 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.

Contents

Foreword

This part of NRS 009 has been prepared on behalf of the Electricity Suppliers Liaison Committee (ESLC) and has been approved by it for use by supply authorities.

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 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*
- *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 0-626-12165-5

This part of NRS 009 was accepted by a Working Group which comprised the following members:

P A Johnson (Chairman)	NRS Project
V Bissett	Cape Town Municipality
L D M de Wet	City Council of Boksburg
J A Ehrich	Pretoria Electricity Department
E Joubert	Benoni City Council, Electricity Department
J O'Kennedy	Eskom (Electrification)
V Patel	Durban Electricity
V E Rengecas	SABS
WCG Terblanche (Project Leader)	Y2K Solutions Africa
S J van den Berg	City of Bloemfontein, Electricity Department
D W van Reenen	Johannesburg Electricity

This part of NRS 009 was compiled using the contents of Part 2B of the standard transfer specification (STS). The working group acknowledges the contribution of G R McKay of Prism Payment Technologies (Pty) Ltd as the compiler of Part 2b of the STS for Eskom. The intellectual property rights to the STS have been ceded to the STS Association (see the notice at the front of this part of NRS 009).

The Working Group was appointed by the ESLC, which, at the time of approval, comprised the following members:

R Wienand (Chairman)	Durban Transitional Metropolitan Council, AMEU
H D Beck	East London Municipality
M N Bailey	Eskom (Distribution Technology)
A J Claasen	Manager, Electrical Engineering Standards, SABS
F H D Conradie	Eskom (Transmission)
P Crowdy	Eskom (Distribution Technology)
J A Ehrich	City Electrical Engineer, Pretoria, AMEU
P A Johnson	Corporate Technology Standardization Manager, Eskom
D A Kruger	Chamber of Mines
I P Kruger	Director, Department of Electrical Engineering, SABS
J G Louw	Tygerberg City
D M Michie	City Electrical Engineer, Port Elizabeth, AMEU
G Munro	City Electrical Engineer, Cape Town, AMEU
A J van der Merwe	City Electrical Engineer, Bloemfontein, AMEU
P J S van Niekerk	Greater Johannesburg Metropolitan Electricity
H R Whitehead	Executive Director, Durban 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.

Introduction

This part of NRS 009 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 and sections of NRS 009. Compliance with all the normative (mandatory) requirements of all the following specifications is a requirement in the implementation of an STS-complaint 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 part of NRS 009 is technically the same as Part 2b of the STS specification. An annex has been added to describe the process of key management in a flow diagram.

Key words

Standard Transfer Specification; Interface; Metering; Pre-payment; Credit dispenser; Electricity dispenser; Key management; Cryptographic keys.

SPECIFICATION

Electricity sales systems

Part 7: Standard transfer specification/Management of cryptographic keys

Requirements for applications in the Electricity Supply Industry

1 Scope

1.1 This part of NRS 009 specifies the management of standard transfer specification (STS) cryptographic keys utilized by the STS cryptographic algorithm 1 to secure the transfer of STS token data from credit dispensers to electricity dispensers that support STS version 1.0.

1.2 It specifies the various types of key used and, for each key type, its purpose, relationship to other key types, method of generation and method of changing key values.

NOTE The distribution of information and equipment that require key management processes, is illustrated in annex A.

1.3 This part of NRS 009 is intended for application by manufacturers of devices that input or output STS-compliant tokens, and in particular manufacturers of electricity dispensers or credit dispensers that support STS version 1.0.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of NRS 009. 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 part of NRS 009 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.

ANSI X3.92:1981, *Data encryption algorithm (DEA).*

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

NRS 009-4-1:1994, *Electricity sales systems – Part 4: National electricity meter cards and associated numbering standards – Section 1: National electricity meter cards.*
(Amendment 1, 1996)

NRS 009-4-2:1993, *Electricity sales systems – Part 4: National electricity meter cards and associated numbering standards – Section 2: National electricity meter numbers.*
(Amendment 1, 1996)

NRS 009-6-6:1998, *Electricity sales systems – Part 6: Interface standards – Section 6: Standard transfer specification/Credit dispensing unit – Electricity dispenser – Categories of token and transaction data fields.*

NRS 009-6-7:1999, *Electricity sales systems – Part 6: Interface standards – Section 7: Standard transfer specification/Credit dispensing unit – Electricity dispenser – Token encoding and data encryption and decryption.*

NRS 009-6-8:1998, *Electricity sales systems – Part 6: Interface standards – Section 8: Standard transfer specification/Disposable magnetic token technology – Token encoding format and physical token definition.*

NRS 009-6-9:1998, *Electricity sales systems – Part 6: Interface standards – Section 9: Standard transfer specification/Numeric token technology – Token encoding format and physical token definition.*

3 Terms, definitions and abbreviated terms

For the purpose of this specification, the definitions given in SABS 1524-0 and the following apply:

3.1 Terms and definitions

3.1.1 algorithm: A precise and rigorous statement of a method of calculation.

3.1.2 authentication: A process used between a sender and a receiver to ensure data integrity and origin integrity.

3.1.3 child key: A key that is encrypted with a parent key.

3.1.4 cipher: A method of cryptography that applies an algorithm to the letters or digits of the plaintext to create ciphertext, and vice versa.

NOTE Typically the algorithm is used in conjunction with one or more keys.

3.1.5 common group: See common supply group (3.1.6).

3.1.6 common supply group: A supply group that associates a set of electricity dispensers on a geographical or regional basis, in which each and every electricity dispenser in the supply group has a common dispenser key.

3.1.7 cryptographic key: A parameter used in conjunction with an algorithm for the purposes of validation, authentication, encipherment or decipherment.

3.1.8 cryptography: The discipline that embodies the principles, means and methods for the transformation of data in order to conceal its information content, or prevent its undetected modification, or prevent its unauthorized use (or any combination of these).

3.1.9 data integrity: The property that shows that data have not been altered or destroyed in an unauthorized manner.

3.1.10 decipherment: The cryptographic transformation of ciphertext data (see cryptography (3.1.8)) to produce plaintext data; the reversal of encipherment.

3.1.11 decryption: See decipherment (3.1.10).

3.1.12 default group: See default supply group (3.1.13).

3.1.13 default supply group: A supply group that associates a set of electricity dispensers which

have not yet been allocated to a unique supply group or a common supply group, and in which each and every electricity dispenser in the supply group has a unique dispenser key.

3.1.14 dispenser key: A key associated with an electricity dispenser and used together with the standard transfer algorithm to encrypt tokens generated at a credit dispenser and to decrypt tokens input at an electricity dispenser.

3.1.15 electricity dispenser (ED) key register: A physically secure environment for the non-volatile storage of the electricity dispenser's current dispenser key.

3.1.16 encipherment: The cryptographic transformation of plaintext data (see cryptography (3.1.8)) to produce ciphertext data.

3.1.17 encryption: See encipherment (3.1.16).

3.1.18 exclusive-or addition: See modulo-2 addition (3.1.27).

3.1.19 interoperability: The ability to exchange keys, whether manually or automatically, between equipment supplied by one manufacturer and operated by one party and equipment supplied by another manufacturer and operated by another party.

3.1.20 key activation date: An attribute associated with a vending key value that defines the date upon which the vending key becomes the supply group's current vending key, and the date upon which the associated key revision number becomes the supply group's key revision number.

3.1.21 key block: In the context of the standard on data encryption (ANSI X3.92), the 64 bit block of data that contains the 56 bit key.

3.1.22 key expiry number: An attribute associated with a key value that defines the period during which the key value can be used.

NOTE 1 A token that is encrypted with a key whose token identifier exceeds the electricity dispenser's key expiry number for the key will be rejected by the electricity dispenser.

NOTE 2 Implementation of key expiry is optional for an electricity dispenser.

3.1.23 key revision number: An attribute associated with a key value and that provides a key sequencing identifier.

3.1.24 key type: An attribute associated with a key value and that defines the purpose for which the key value can be used.

3.1.25 magnetic card electricity dispenser: An electricity dispenser that incorporates magnetic card token technology as the mechanism for inputting standard transfer specification tokens.

3.1.26 magnetic card token technology: A technology that enables entry, by a human, of a standard transfer specification disposable magnetic card token into a device via a magnetic card reader.

3.1.27 modulo-2 addition: A binary addition with no carry, giving the following values:

0 + 0 = 0;
0 + 1 = 1;
1 + 0 = 1;
1 + 1 = 0.

3.1.28 one-way function: A function $y = f(x)$ that is relatively easy to compute, but the inverse of which is much more difficult to compute (in other words, given x, it is easy to find y, but given a value y it is difficult to find any solution x of $y = f(x)$).

3.1.29 origin integrity: The corroboration that the source of data received is as claimed.

3.1.30 parent key: A key used to encrypt a child key for the purpose of concealing the child key, in order to prevent its undetected modification or unauthorized use (or both).

3.1.31 physically secure environment: An environment in the form of a facility, enclosure or device the penetration of which, in any manner, actively renders unintelligible any secret data contained therein, or that itself precludes any penetration that could allow disclosure of secret data.

3.1.32 seed key: A key used by an algorithm as a starting or initializing value for the generation of another value.

3.1.33 supply group key revision number: An attribute of a supply group and that defines the current key revision number for the supply group, and therefore the current vending key value for the supply group (see also key revision number (3.1.23)).

3.1.34 token identifier: A value associated with a token and that distinguishes the token from other tokens issued for the same electricity dispenser.

NOTE The token identifier is derived from the date and time the token is issued at the credit dispenser.

3.1.35 unique group: See unique supply group (3.1.36).

3.1.36 unique supply group: A supply group that associates a set of electricity dispensers on a geographical or a regional basis, in which each and every electricity dispenser in the supply group has a unique dispenser key.

3.1.37 validation: The process of checking the data integrity of a message, or selected parts of a message.

3.2 Abbreviated terms

The following abbreviations are used in this standard:

3.2.1 ANSI: American National Standards Institute

3.2.2 CDU: credit dispensing unit

3.2.3 CRC: cyclic redundancy code

3.2.4 CVS: common vending system

3.2.5 DCTK: dispenser common standard transfer specification key

3.2.6 DDTK: dispenser default standard transfer specification key

3.2.7 DEA: data encryption algorithm

3.2.8 DES: data encryption standard

3.2.9 DITK: dispenser initialization standard transfer specification key

3.2.10 DUTK: dispenser unique standard transfer specification key

3.2.11 ECB: electronic code book

3.2.12 ED: electricity dispenser

3.2.13 EDDK: electricity dispenser data encryption standard key

3.2.14 EDIB: electricity dispenser input block

3.2.15 ODDP: odd parity function

3.2.16 OWF: one way function

3.2.17 PAN: primary account number

3.2.18 STA: standard transfer algorithm

3.2.19 STS: standard transfer specification

3.2.20 VCDK: vending common data encryption standard key

3.2.21 VDDK: vending default data encryption standard key

3.2.22 VUDK: vending unique data encryption standard key

4 Requirements

4.1 STS key types

4.1.1 General

STS keys are classified according to STS key types (see 3.1.2.4). The following four STS key types are defined:

a) dispenser initialization STS key (DITK) – key type 0;

b) dispenser default STS key (DDTK) – key type 1;

c) dispenser unique STS key (DUTK) – key type 2; and

d) dispenser common STS key (DCTK) – key type 3.

For the purpose of this specification, an electricity dispenser (ED) is presumed to be capable of storing at least one STS key value and its associated key type. This key storage area is referred to as the ED key register (see 3.1.15).

A description of each key type and its relationship to other key types is given in 4.1.2 to 4.1.6.

4.1.2 Dispenser initialization STS key type 0 (DITK)

4.1.2.1 Keys of type 0 are used to initialize the ED key register during production or repair at the manufacturer's premises. These keys are the property of the ED manufacturer. As such, they are generated and managed by the manufacturer, and are unknown to the electricity supplier. They do not form part of the common vending system (CVS), and no manufacturer's DITK values are managed by or known to the CVS.

4.1.2.2 No ED purchased by the electricity supplier shall leave a manufacturer's site with a DITK value in the ED key register. The ED key register shall contain either a DDTK, DUTK or DCTK value supplied by the electricity supplier. A DITK is the only key type that can be introduced into an ED as a plaintext value; DDTK, DUTK or DCTK values can only be introduced into an ED as ciphertext (encrypted) values.

4.1.2.3 A DITK shall only be used for the following key management functions:

a) as the parent key for another DITK; in other words, to encrypt another DITK for the purpose of introducing it into the ED key register;

b) as the parent key for a DDTK;

c) as the parent key for a DUTK; and

d) as the parent key for a DCTK, but only in a magnetic card ED.

4.1.2.4 The functions in 4.1.2.3 (a) to (d) may be performed via the STS set dispenser key functions with STS tokens (see NRS 009-6-7), or via a manufacturer proprietary loading mechanism that utilizes the STS set dispenser function data. The ED should only accept the DDTK, DUTK or DCTK encrypted under the DITK supplied by the manufacturer in the set dispenser key token format.

4.1.2.5 It is the responsibility of the manufacturer to ensure that appropriate security measures are applied to any DITK so that DDTK, DUTK or DCTK values encrypted with a DITK cannot be compromised.

4.1.2.6 A DITK can also be used to decrypt other dispenser-specific management functions, (see NRS 009-6-7). It can be used to decrypt an STS credit transfer function; in other words, a valid STS credit transfer token can be decrypted and applied by an ED that contains a type 0 key in its key register in order to facilitate testing of the ED during production or repair.

4.1.3 Dispenser default STS key type 1 (DDTK)

4.1.3.1 Keys of type 1 are used to support EDs allocated to default supply groups. An ED that has not been allocated to a common supply group or a unique supply group at the time of manufacture or repair cannot be loaded with its corresponding DCTK or DUTK value. Instead it is allocated to a default group and loaded with its corresponding DDTK value, encrypted under a parent DITK. Subsequently, at the time of installation or operation, an ED that has been re-allocated to a default group can be loaded with the corresponding DDTK value, encrypted under a parent DDTK, DUTK or DCTK.

4.1.3.2 A DDTK is a secret value, and shall not be accepted by an ED as a plaintext value; it shall only be loaded by an ED if encrypted under the parent key present in the EDs key register. DDTK values are the property of the respective utility. As such, they form part of the CVS, are managed by the respective utility, and are unknown to the manufacturer. An ED purchased by the electricity supplier, or one of its distributors, which leaves a manufacturer's site may contain a DDTK value supplied by the utility in the ED key register.

4.1.3.3 A DDTK shall only be used for the following key management functions:

a) as the parent key for another DDTK; in other words, to encrypt another DDTK for the purpose of introducing it into the ED key register;

b) as the parent key for a DUTK; and

c) as the parent key for a DCTK, but only in a magnetic card ED.

4.1.3.4 The functions in 4.1.3.3 (a) to (c) may be performed via the STS set dispenser key functions with STS tokens, or via a manufacturer's proprietary loading mechanism that utilizes the STS set dispenser function data. A DDTK shall not be used to decrypt a DITK for the purpose of introducing it into the ED key register.

4.1.3.5 A DDTK can also be used to decrypt other dispenser-specific management functions (see NRS 009-6-7). It shall not be used to decrypt an STS credit transfer function; in other words, a valid STS credit transfer token shall not be decrypted and applied by an ED that contains a key of type 1 in its key register, even if the STS credit transfer token has been encrypted with the same DDTK value.

4.1.4 Dispenser unique STS key type 2 (DUTK)

4.1.4.1 Keys of type 2 are used to support EDs allocated to unique supply groups. An ED that has been allocated to a unique supply group at the time of manufacture or repair can be loaded with its DUTK value that corresponds to the unique group and that has been encrypted under a parent DITK. Subsequently, at the time of installation or operation, an ED which has been re-allocated to a unique group can be loaded with the corresponding DUTK value, encrypted under a parent DDTK, DUTK or DCTK.

4.1.4.2 A DUTK is a secret value, and shall not be accepted by an ED as a plaintext value. It shall only be loaded by an ED if it has been encrypted under the parent key present in the EDs key register. DUTK values are the property of the respective utility. As such, they form part of the CVS, are managed by the respective utility, and are unknown to the manufacturer. An ED purchased by the electricity supplier, or one of its distributors, and that leaves the manufacturer's site may contain a DUTK value supplied by the utility in the ED key register.

4.1.4.3 A DUTK shall only be used for the following key management functions:

a) as the parent key for another DUTK; in other words, to encrypt another DUTK for the purpose of introducing it into the ED key register; and

b) as the parent key for a DDTK.

4.1.4.4 The functions in 4.1.4.3 (a) and (b) may be performed via the STS set dispenser key functions with STS tokens, or via a manufacturer's proprietary loading mechanism that utilizes the STS set dispenser function data. A DUTK shall not be used to decrypt a DITK or a DCTK for the purpose of introducing it into the ED key register.

4.1.4.5 A DUTK can also be used to decrypt other dispenser-specific management functions (see NRS 009-6-7). It can be used to decrypt a STS credit transfer function; in other words, a valid STS credit transfer token can be decrypted and applied by an ED that contains a key of type 2 in its key register.

4.1.5 Dispenser common STS key type 3 (DCTK)

4.1.5.1 Keys of type 3 are used to support magnetic card EDs allocated to common supply groups. A magnetic card ED that has been allocated to a common group at the time of manufacture or repair can be loaded with the DCTK value that corresponds to the common group and that has been encrypted under a parent DITK. Subsequently, at the time of installation or operation, a magnetic card ED that has been re-allocated to a common group can be loaded with the corresponding DCTK value that has been encrypted under a parent DDTK or DCTK.

4.1.5.2 A DCTK can only be used with magnetic card token technology (token technology code 01), and shall only be accepted by a magnetic card ED. It shall not be used with any other type of token technology, and shall be rejected by any other type of token technology ED.

4.1.5.3 A DCTK is a secret value, and shall not be accepted by an ED as a plaintext value; it shall only be loaded by an ED if it has been encrypted under the parent key present in the EDs key register. DCTK values are the property of the respective utility. As such, they form part of the CVS, are managed by the respective utility and are unknown to the manufacturer. A magnetic card ED purchased by the electricity supplier, or one of its distributors, and that leaves the manufacturer's site may contain a DCTK value supplied by the utility in the ED key register.

4.1.5.4 A DCTK shall only be used for the following key management functions:

a) as the parent key for another DCTK; in other words, to encrypt another DCTK for the purpose of introducing it into the ED key register;

b) as the parent key for a DDTK; and

c) as the parent key for a DUTK.

4.1.5.5 The functions in 4.1.5.4 (a) to (c) may be performed via the STS set dispenser key functions with STS tokens, or via a manufacturer's proprietary loading mechanism that utilizes the STS set dispenser function data. A DCTK shall not be used to decrypt a DITK for the purpose of introducing it into the ED key register.

4.1.5.6 A DCTK can also be used to decrypt other dispenser-specific management functions, (see NRS 009-6-7). It can be used to decrypt a STS credit transfer function; in other words, a valid STS credit transfer token can be decrypted and applied by a magnetic card ED that contains a key of type 3 in its key register.

4.1.6 STS key type relationships

Figure 1 illustrates the key type relationships as a hierarchy. Where one key is used to encrypt another key (as in the set 1st and 2nd section dispenser key token pair), the former is referred to as the parent key (see 3.1.30), and the latter as the child key (see 3.1.3). The arrows denote the purpose for which a key type can be used, i.e. the values that may encrypt or decrypt. At the arrow tail is the parent STS key type, and at the arrow head the child STS key type or STS function, for example, only a DITK, DUTK or DCTK can be used to encrypt or decrypt a credit transfer function, but all four key types can be used to encrypt or decrypt dispenser-specific management functions.

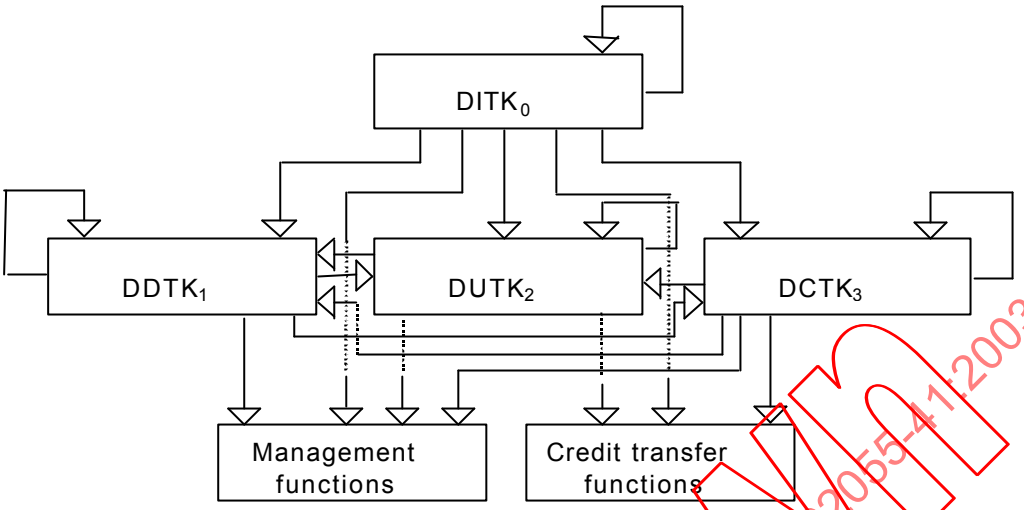


Figure 1 – Relationships among STS key types

Table 1 details the permitted relationships in tabular form. The child key rows refer to the permitted usage of dispenser key types for encryption of dispenser keys in the set 1st and 2nd section dispenser key management functions. Similarly, the management and credit rows detail the permitted usage of dispenser key types for the encryption of the remaining dispenser-specific management functions and credit transfer functions respectively.

Table 1 – Permitted relationships among STS key types

1	2	3	4	5
Child key	**Permitted usage**			
	Parent key			
	$DITK_0$	$DDTK_1$	$DUTK_2$	$DCTK_3$
$DITK_0$	Yes	No	No	No
$DDTK_1$	Yes	Yes	Yes	Yes[a]
$DUTK_2$	Yes	Yes	Yes	Yes[a]
$DCTK_3$	Yes[a]	Yes[a]	No	Yes[a]
Function				
Management	Yes	Yes	Yes	Yes[a]
Credit	Yes	No	Yes	Yes[a]
[a] For magnetic card ED only.				

4.2 Vending key types

A vending key is a DES key value that is secretly generated, stored and distributed within the CVS. DES vending keys are the CVS seed keys from which STS dispenser keys are generated.

Vending keys are classified according to vending key type. The key type is an attribute of the key that defines the purpose for which the key can be used. Three vending key types are defined and correspond to the three types of supply group, namely default, unique and common. The vending key for a given supply group is the seed key used to generate the dispenser keys for all EDs within the supply group:

a) vending default DES key (VDDK) the seed key type for generation of type 1 (DDTK) key values – it shall not be used to generate type 0 (DITK), type 2 (DUTK) or type 3 (DCTK) key values;

b) vending unique DES key (VUDK) the seed key type for generation of type 2 (DUTK) key values – it shall not be used to generate type 0 (DITK), type 1 (DDTK) or type 3 (DCTK) key values; and

c) vending common DES key (VCDK) the seed key type for generation of type 3 (DCTK) key values – it shall not be used to generate type 0 (DITK), type 1 (DDTK) or type 2 (DUTK) key values.

At any given moment, a unique VDDK value exists for each default group defined in the CVS. Similarly, a unique VUDK value for each unique group and a unique VCDK value for each common group are defined.

4.3 STS key generation

With the exception of type 0 (DITK) key values, STS key values shall only be generated by a device responsible for token generation, such as a CVS CDU that is certified as STS compliant and which is subject to STS key management. This section describes the STS key generation method used by such devices, and is applicable to manufacturers of these devices. It is not applicable to ED manufacturers.

4.3.1 Overview

A STS key for an ED is generated as output from a one-way function with two inputs, namely a vending-key-related input and an ED-related input. The vending key has a secret DES key value (see ANSI X3.92), generated and maintained within the CVS. At any given moment, a unique vending key value exists for each supply group (whether default, unique or common) defined within the CVS.

The ED input data consist of the ED's supply group code, tariff index, key revision number and primary account number (PAN). For an ED allocated to a common group, the ED PAN is not used. Instead the ED number portion of the PAN input is set to zeroes (giving a PAN of 600727000000000009 for a PAN issuer code of 600727). As a result, all EDs in a common group that share the same tariff index and key revision number share a common ED input, irrespective of their different ED numbers.

Only STS type 1 (DDTK) and type 2 (DUTK) key values can therefore be generated from a vending key value and an ED value unique to a particular ED. A type 0 (DITK) key value is generated and maintained by the ED manufacturer in accordance with a manufacturer-specific and proprietary technique.

Two STS key generation algorithms are defined, and the second supercedes the first. The first algorithm (referred to as algorithm 1a) should only be used for an ED with a key revision number of 1, the ED number of which occurs within a prescribed set of ED number ranges. The second algorithm (referred to as algorithm 1b) should be used for an ED with a key revision number of 2 to 9. Where the number of an ED falls within the prescribed range and the STS key of the ED is changed from revision 1 to revision 2, the revision 2 key is generated using algorithm 1b and the revision 1 key is generated using algorithm 1a.

4.3.2 Notation

The following notation is used:

a) DES algorithm (see ANSI X3.92):

1) DES key dk: any general reference to a DES key is denoted dk. Any particular DES key label ends with dk, for example, EDDK denotes electricity dispenser DES key

2) encryption with dk: DES algorithm ECB mode encryption of plaintext *x* with key dk resulting in ciphertext *y* is denoted $y = DEA1^{+}_{dk}(x)$

3) decryption with dk: DES algorithm ECB mode decryption of ciphertext *y* with key dk resulting in plaintext *x* is denoted $x = DEA1^{-}_{dk}(y)$

b) STS algorithm (see NRS 009-6-7):

1) STS key tk: any general reference to a STS key is denoted tk. Any particular STS key label ends with tk, for example, DDTK denotes dispenser default STS key

2) encryption with tk: STS algorithm encryption of plaintext *x* with key tk resulting in ciphertext *y* is denoted $y = STA1^{+}_{tk}(x)$

3) decryption with tk: STS algorithm decryption of ciphertext *y* with key tk resulting in plaintext *x* is denoted $x = STA1^{-}_{tk}(y)$

c) Exclusive-or addition: the exclusive-or or modulo-2 addition of values *w* and *x* resulting in *y* is denoted $y = x +_2 w$

d) Odd parity operation: transforming a 56 bit DES key npdk with no parity to a 64 bit DES key block opdk with odd parity is denoted by opdk = ODDP(npdk).

A 56 bit DES key is expanded to an odd parity 64 bit DES key block by means of the standard convention of inserting an odd parity bit after every successive 7 key bits; in other words, there are an odd number of bits in every byte of the 8 byte or 64 bit vending DES key block output:

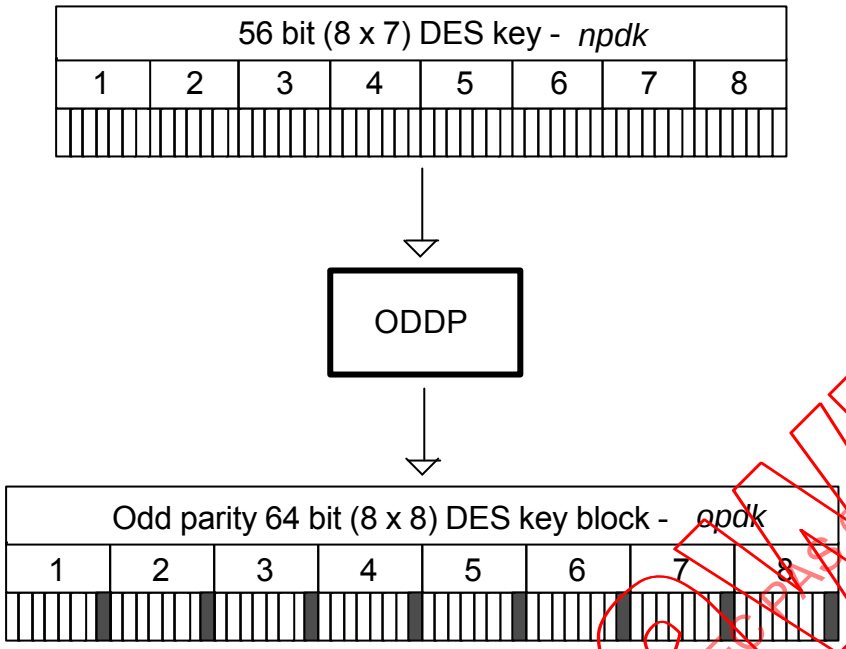


Figure 2 – Odd parity function ODDP

4.3.3 ED input block

Both algorithms make use of a 64 bit ED input block, made up from the following ED-related data:

a) supply group code;

b) tariff index;

c) key revision number; and

d) PAN;

and the key type as defined in 4.1.

Using the following notation:

C Control field digit:

Let: $c^3c^2c^1c^0$ denote the binary values of the four control field bits:

c^3 Reserved for future use. Always zero

c^2 Reserved for future use. Always zero

c^1c^0 STS key type:

00 Key type 0: DITK

01 Key type 1: DDTK

10 Key type 2: DUTK

11 Key type 3: DCTK

S Supply group code digit. Range 0_{16} to 9_{16}

T Tariff index digit. Range 0_{16} to 9_{16}

R Key revision number digit. Range 0_{16} to 9_{16}

F Pad value digit. Always F_{16}

D ED PAN digit. Range 0_{16} to 9_{16}

where

n_{16} denotes a hexidecimal number.

Construct two 64 bit blocks, the control block and PAN block, shown in hexadecimal format, with the most significant digit in position 1 and the least significant digit in position 16.

Control block:

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Value	C	S	S	S	S	S	S	T	T	R	F	F	F	F	F	F

PAN block:

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Value	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D

For default and unique group EDs, the ED PAN digits input to the PAN block are the least significant (right-most) 16 digits of the PAN, excluding the PAN check digit (note that the dispenser number check digit is included). The least significant PAN digit extracted is in position 16, and the most significant digit extracted is in position 1. If the PAN is of insufficient length to make up the 16 digits, the digits extracted are right justified within the block and padded to the left with zeroes (for example, for a PAN issuer code of 600727 and an ED number of 12345678903, the PAN is 600727123456789030 and the PAN block is 0072712345678903).

For a common group ED, the actual ED PAN is ignored and the ED number portion of the PAN is set to zeroes (for example, for a PAN issuer code of 600727, the PAN block is 0072700000000000).

Perform an exclusive-or operation on the control block and the PAN block to yield a single 64 bit ED input block (EDIB):

EDIB = CONTROL BLOCK $+_2$ PAN BLOCK

4.3.4 Algorithm 1a

4.3.4.1 One-way function

A one-way function denoted by OWF is defined as follows:

$y = OWF_{dk}(x) = DEA1^{+}_{dk}(x) +_2 x$

This is depicted in figure 3.

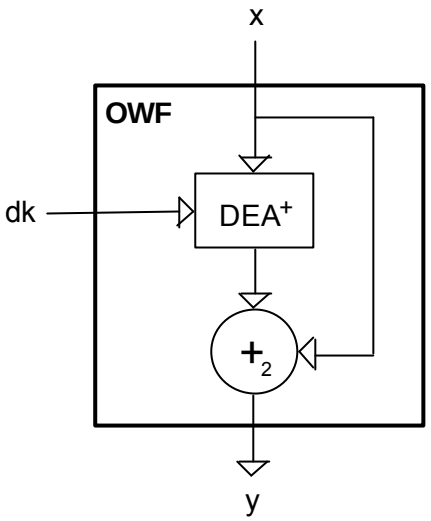


Figure 3 – One-way function (OWF)

4.3.4.2 Key generation algorithm 1a

The generation of the dispenser STS key for an ED from a vending DES key and ED-related data makes use of the one-way function defined in 4.3.4.1 and the ED input block defined in 4.3.3:

$y = OWF_{dk}(x)$

The OWF input x is obtained from the vending DES key (VDDK, VUDK or VCDK). The 56 bit vending DES key is expanded to a 64 bit vending DES key block using the standard odd parity convention and operation:

x = ODDP(VDDK), or x = ODDP(VUDK), or x = ODDP(VCDK).

The OWF key dk (EDDK) is obtained from the ED input block EDIB defined in 4.3.3. Only the leftmost 7 bits of every successive byte of the 8 bytes form the actual 56 bit DES key value; the 8th least significant bit (i.e. the parity bit position) of each successive byte in the 64 bit key block is ignored. This 56 bit value is the DES key for the ED (EDDK) to be substituted in the one way function as dk. The resultant dispenser STS key value is generated from the one-way function defined in 4.3.5.1:

For a vending default key:

$DDTK = OWF_{EDDK}$ (ODDP(VDDK))

Similarly, for a vending unique key:

$DUTK = OWF_{EDDK}$(ODDP(VUDK))

and for a vending common key:

$DCTK = OWF_{EDDK}$(ODDP(VCDK))