DOCUMENT HISTORY

AUTHOR	REVISION	DATE	DOCUMENT TYPE
Roy Kaplan	1	10/05/95	Draft

Document prepared by: ***Measurement and Control Department,***
National PTM&C,
Transmission Group,
Eskom

Approval :

Design Engineer	*Section Manager*	*M&C Manager*

STANDARD TRANSFER SPECIFICATION

GUIDELINES

Definitions

The following definitions are relevant For the purpose of this standard the following definitions apply:

agent: Party responsible for the operation and management of *credit dispensers* at *point of sale* locations in support of the sale of pre-paid electricity *tokens* to *customers* on behalf of *distributors*.

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

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

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

cipher: A method of *cryptography* which applies an *algorithm* to the letters or digits of the *plaintext* to create *ciphertext*, and vice versa. Typically the *algorithm* is used in conjunction with one or more *keys*.

ciphertext: The enciphered form of data (see *cipher*, *encipherment*).

common group: See *common supply group*.

common supply group: A *supply group* associating 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*.

credit dispenser: A device capable of generating standard transfer specification *tokens* for the transfer of management and credit information to an *electricity dispenser*.

credit dispensing unit: See *credit dispenser*.

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

cryptography: The discipline which embodies principles, means and methods for the transformation of data in order to conceal its information content, prevent its undetected modification and/or prevent its unauthorised use.

customer: Party residing at or representing a site at which a *distributor's electricity dispenser* is installed, who purchases a pre-paid electricity token from a *credit dispenser*.

data integrity: The property that data has not been altered or destroyed in an unauthorised manner.

decipherment: The cryptographic transformation of *ciphertext* data (see *cryptography*) to produce *plaintext* data - the reversal of *encipherment*.

decryption: See *decipherment*.

default group: See *default supply group*.

default supply group: A *supply group* associating a set of *electricity dispensers* which are not yet allocated to a *unique supply group* or *common supply group*, in which each and every electricity dispenser in the supply group has a unique *dispenser key*.

dispenser card: An identification card uniquely associated with an *electricity dispenser*, issued by the *distributor* and used by the *customer* during a *vending transaction* to provide dispenser specific identification and management data required by the *credit dispenser* to output a *token* that may be input to the electricity dispenser.

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 decrypt tokens input at an electricity dispenser.

distributor: A party responsible for the installation, connection, operation and management of *electricity dispensers* at *customer* sites in support of the supply of electricity via the distribution network.

electricity dispenser: A device capable of inputting standard transfer specification management and credit *tokens*, and executing functions according to the information on the token, including the metering of electricity.

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

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

encryption: See *encipherment*.

exclusive-or: See *modulo-2 addition*.

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.

key: Abbreviated term for *cryptographic key*.

key activation date: An attribute associated with a *vending key* value which 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 key revision number*.

key block: In the context of the Data Encryption Standard (ANSI X3.92), it is the 64 bit block of data which contains the 56 bit *key*.

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

key management: ???

key revision number: An attribute associated with a *key* value which provides a key sequencing identifier.

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

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

magnetic card token technology: A technology which enables the human entry of a standard transfer specification disposable magnetic card *token* into a device via a magnetic card reader.

manufacturer: A party involved in the design and/or development and/or production of *electricity dispensers* and/or *credit dispensers*.

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.

one-way function: A function *y=f(x)* which is relatively easy to compute, whose inverse is much more difficult to compute (i.e. 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)*).

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

parent key: A *key* used to encrypt a *child key* for the purpose of concealing the child key, preventing its undetected modification and/or unauthorised use.

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

plaintext: Data which is not in an enciphered state (see *cipher, encipherment*) and is therefore in its normal form.

point of consumption: *Customer* location at which an *electricity dispenser* installed and operated by a *distributor* is situated in support of the metered supply of electricity according to the amount of electricity input from a pre-paid electricity *token*.

point of sale: Location at which a *credit dispenser* operated by an *agent* is situated in support of the sale of pre-paid electricity *tokens* to *customers*.

secrecy: ???

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

supply group: A classification used by *distributors* for the purpose of grouping *electricity dispensers*, thereby facilitating their management and control. Three types of supply group are defined - *default supply group*, *unique supply group* and *common supply group*.

supply group key revision number: An attribute of a *supply group* which defines the current *key revision number* for the supply group, and therefore the current *vending key* value for the supply group.

token: A data transport mechanism carrying a data message defined according to the standard transfer specification for the transfer of management and credit information between a *credit dispenser* and an *electricity dispenser*.

token technology: ???

unique group: See *unique supply group*.

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

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

vending key: A *key* associated with a *supply group* and used as a *seed key* to generate *dispenser keys* for *electricity dispensers* in the supply group.

vending system: A system utilised by an *agent* for the operation and management of *credit dispensers* at *point of sale* locations in support of the sale of pre-paid electricity *tokens* to *customers* on behalf of *distributors*.

vending transaction: A transaction uniquely associated with an *electricity dispenser*, *credit dispenser* and *token* which records all relevant information pertaining to the purchase of the pre-paid electricity token by a *custome*r from the *agent's* credit dispenser to activate the supply of electricity from the *distributor's* electricity dispenser.

Abbreviations

The following abbreviations are used in this standard:

Abbreviation	Meaning
CDU	Credit Dispenser Unit
CRC	Cyclic Redundancy Check/Code
CVS	Common Vending System
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
ED	Electricity Dispenser
ISO	International Organization for Standardization
OWF	One Way Function
PAN	Primary Account Number
POC	Point Of Consumption
POS	Point Of Sale/Service
STA	Standard Transfer Algorithm
STS	Standard Transfer Specification

STS origins

Historically in electrification pre-payment, the focus of specification and standardization by distributors was on the ED, rather than on the vending system and infrastructure required to support the ED. Typically the specification and development of vending systems was left to the various ED manufacturers. As a result, different vending systems were developed and these were not usually compatible with each other.

The most significant consequence of this incompatibility was the inability of the vending system of one manufacturer to vend to the ED of another. Consequently, a distributor purchasing EDs from different manufacturers had to purchase separate vending systems to support the sale of pre-payment to each manufacturer's ED. This proved to be expensive, inefficient and operationally inconvenient and complex.

Eskom as a major purchaser of EDs initiated the definition of STS as a means of ensuring that the electricity pre-payment tokens output from a CDU developed by one manufacturer could be input to an ED developed by another manufacturer. Separately but in concert with the STS definition process, Eskom defined and developed the CVS to provide a total electricity dispensing system capable of supporting the widespread deployment of pre-payment EDs sourced from a number of different manufacturers. In this regard, it should be emphasized that the STS is a standard, whereas the CVS is a system implemented according to a set of standards.

STS is therefore significant in that it represents the equivalent of an "open systems" standard in the electricity dispensing industry, allowing STS compatible dispensing and vending equipment from different manufacturers to interoperate to the benefit of the customer, distributor and agent, thereby providing a basis for a more competitive, cost-efficient and convenient electricity pre-payment service.

STS general concepts

Introduction

The STS is based upon a number of concepts, a clear appreciation of which significantly eases the task of implementing a CDU or ED. Whilst the STS standards incorporate the majority of information required, not all of these concepts are directly addressed in the STS standards themselves, some being the subject of other specifications or standards applicable to related areas such as the CVS.

Tokens

The standardization of tokens by the STS provides the fundamental basis for achieving the primary objective motivating development and implementation of the STS - to enable ED users to purchase EDs from a variety of manufacturers with the knowledge that these EDs are capable of interoperating with multiple vending systems and CDs which also support the STS standard.

The token provides the data transport mechanism for the transfer of management and credit information between the CDU and ED. The STS standardizes on the following with respect to the token:

- the set of **token functions** that can be transferred via the token for execution by the ED;

- the set of **token data fields** required by the CDU to support the various token functions ;

- the **token formats** corresponding to the various token functions ;

- the **token encryption** of formatted *plaintext* token data into *ciphertext* token data and **token decryption** of ciphertext token data into plaintext token data;

- the **token technologies** that can be used to support the transfer of token data from CDU to ED;

- the **token encoding** of token data onto each of the token technologies.

Token functions

STS defines the set of functions which can be selected at the CDU and transferred via a token to be executed at the ED. Of these, certain are **mandatory** and must be supported by the ED if it is to be STS compliant, and others are **optional** and can be supported by the ED at the implementors discretion. Token functions are either **dispenser specific** or **non-dispenser specific**. Dispenser specific tokens are generated by the CDU in such a manner that they can only be processed by a specific or designated ED or group of EDs. Non-dispenser specific tokens are generated so that they can be processed by any ED supporting the token technology.

These token functions are classified into three **categories**:

- **Credit transfer token functions**. These support the transfer of credit information from a CDU to a specific ED or group of EDs. All credit transfer token functions are dispenser specific, so that credit purchased by a customer can only be input to the ED or EDs for which it is intended. This is critical if there is to be financial and dispensing integrity in the system between agents and distributor;

- **Non-dispenser specific management token functions**. These support the transfer of management information from a CDU to any ED. As classified, these are all non-dispenser specific - i.e. once created, the token can be re-used at any ED by installation or maintenance personnell to perform various standard ED tests;

- **Dispenser specific management token functions**. These support the transfer of management information from a CDU to a specific ED or group of EDs. As classified, these are all dispenser specific;

Token formats

STS defines the format of each token. All tokens in the standard are 66 bits in length. The basic **structure** of this 66 bits is identical for each token format. The 2 bit **class** (category) and 4 bit **sub-class** uniquely identify the token function, and in turn define the token format and token data required. The remainder of each token consists of 44 bits of **token data** and 16 bits of **checksum** calculated over the preceding 50 bits. This checksum enables the ED to verify the *data integrity* of the token.

Just as the basic structure for all tokens is identical, the structure of the token data within each class is, with minor exception, also identical.

- **Class 00 - credit transfer functions**;
- **Class 01 - non-dispenser specific management**;
- **Class 02 - dispenser specific management functions**.

Token encryption and decryption

Encryption provides the means for ensuring that a token is secured during the transfer from CDU to ED. The token is encrypted at the CDU prior to encoding and transfer to the ED, where it is decrypted.

For credit transfer function tokens (class 00) and dispenser specific management function tokens (class 10), the rightmost 64 bits (i.e. excluding the 2 bit token class) are encrypted after formatting and transferred as ciphertext. For non-dispenser specific management function tokens, the 66 bits are formatted and transferred as plaintext (i.e. these tokens are not encrypted).

Thus credit transfer and dispenser specific management tokens must be decrypted by the ED from ciphertext to plaintext prior to processing.

Token technology and encoding

The token technology defines the technology used to transfer the token data from the CDU to the ED. As such, it also defines a corresponding CDU technology requirement for the CDU to encode the token data onto the token technology, and an ED technology requirement for the ED to decode the token data off the token technology. Two token technologies are defined:

- **Disposable magnetic card token technology** - this transfers the token data on a disposable magnetic stripe card corresponding in shape, dimensions (excluding thickness) and magnetic stripe location with the plastic magnetic stripe card we are familiar with from using credit and other banking cards, except that it is usually constructed from paper rather than plastic and is not intended for reuse.

  The ISO 7810 series of standards upon which the STS disposable magnetic card token technology is based allow for the encoding of three tracks of data on the magnetic stripe, referred to as tracks 1, 2 and 3. Tracks 1 and 2 are standardized by ISO as read only tracks (i.e. write once, read many) and track 3 as a read-write track (i.e. write many, read many).

  The disposable magnetic card token technology utilises the track 3 standard to transport token data. The CDU therefore requires a magnetic stripe track 3 encoder to encode the token data onto the disposable magnetic card, and the ED a magnetic stripe track 3 decoder to idecode the token data off the disposable magnetic stripe card.

- **Numeric token technology** - this transfers the token data as a numeric string of 20 digits. Unlike the disposable magnetic token technology, the physical transport mechanism can vary (for example, it could even be memorised by the customer). Typically, the 20 digit numeric token is printed on the customer receipt, and the physical transport mechanism therefore is paper.

  Whereas the physical transport mechanism of numeric token technology is inherently flexible and can vary, the input mechanism at the ED is always a numeric keypad into which the 20 digit numeric token is keyed.

Supply group

For the purpose of installation, operation and management, each ED is allocated to a *supply group* by the distributor. A supply group is a classification uniquely identified by a *supply group code*, and used by distributors to facilitate the management and control of EDs. Three types of supply group are defined - *unique supply group*, *common supply group* and *default supply group*. Unique and common supply groups correspond to geographical regions. Thus an ED installed at a dwelling in a town is allocated the supply group code corresponding to that of the supply group which geographically incorporates the town.

At the time an STS ED is manufactured, it must be associated with a supply group code and other information required by the STS if it is to be supported by the CVS - however, it is not necessarily known at this stage which supply group the ED will ultimately be allocated to. In this case, the ED is allocated to a default supply group by the CVS. At the time of installation, the CVS transfers the ED from its default supply group to the common or unique supply group corresponding to the actual point of consumption.

Tariff

The vending of electricity at a CDU for an ED requires that the customer be provided with a token containing the number of electricity units corresponding to the amount of electricity purchased. This conversion is governed by an electricity vending *tariff rate*, typically set by the distributor responsible for the ED. The STS caters for a number of tariff rates for each supply group, each identified by a *tariff index*. The CDU uses the supply group code and tariff index (e.g. from the ED magnetic stripe card) to ascertain the appropriate tariff rate for the ED, and applies this to determine the units of pre-paid electricity corresponding to the purchase amount tendered by the customer.

Electricity dispenser identification

Customers purchasing electricity for an ED at a CDU must be able to identify the ED and provide associated information required by the STS. Each ED must be uniquely identified within the vending system by an *ED number* (refer ESKOM MC157), and is issued with an *ED magnetic stripe card* (ESKOM MC115) carrying the ED number, the ED's associated supply group, supply group key revision number and tariff index. The information required for the purchase can be obtained in one of three ways by the CDU - preferably from the ED card if available, from a previous token generated for the ED, or from a customer/ED record maintained by the CDU or the vending system.

STS security and integrity concepts

Introduction

The primary focus of STS security and integrity applies to the token during transfer between the CDU and ED - more specifically to the dispenser specific tokens - credit transfer and dispenser specific management tokens.

In this regard, it is important to ensure that a dispenser specific token:

- can only be accepted by the ED or group of EDs for which it is intended.

  This is part of ensuring a "closed loop" between the distributor supplying the electricity, the agent vending the electricity and the customer consuming the electricity. It would obviously not be satisfactory if a credit transfer token purchased for an ED supplied by distributor A could be used at another ED supplied by distributor B. Distributor B would supply electricity for the amount encoded on the token and not receive funds from the agent, and distributor A would receive the funds without supplying any electricity.

  The specificity of use also has the additional benefit of rendering the token useful to only the customer for which it is intended - by rendering it worthless to others it cannot be resold and theft of the token therefore has no benefit for the thief.

- can only be generated at a CDU authorised to vend for the intended ED.

  This is part of ensuring the "closed loop" previously described, as it ensures that electricity will only be supplied at an ED for tokens which have been legitimately purchased at an authorised CDU - i.e. one where the payment for the token will ultimately be received by the distributor responsible for the ED.

- can only be used once at the intended ED or group of EDs.

  This is obviously imperative if the distributor is not to be defrauded - by using the same credit transfer token more than once (either at the same or different EDs), the distributor would be supplying more electricity than was paid for at the CD.

- cannot be modified during transfer between the CDU and ED.

> Encoded on the credit transfer token is the amount of electricity purchased and paid for at the CD. If this amount could be altered (increased) during transfer, the distributor would supply more electricity to the ED with respect to the vending transaction than it would receive funds from the vending transaction.

All of the above requirements correspond to a well known general security requirement in many data communication scenarios - that of **authenticity**.

Background

Authenticity, secrecy and cryptography

In general, a piece of data, message or file is said to be authentic when it is genuine, came from its reputed source, such source having had the authority to issue it. Authentication is the process adopted in a data communications scenario for ensuring the authenticity of the data communicated.

The secrecy of data should be clearly differentiated from its authenticity. Secrecy ensures that knowledge of the data is restricted to authorised parties - it typically prevents the data against passive attack (eavesdropping) by an adversary. But secrecy of the data does not necessarily prevent against active attack (falsification/altering of data) by an adversary - this is the province of authenticity.

In general, active attack is usually much more complex than passive since there are many different ways of altering data. Among the threats to be considered are:

- alteration, deletion or insertion of data;
- changing the apparent origin of the data;
- changing the actual destination of the data;
- altering the sequence of data;
- using previously transmitted or stored data again (replay).

It can be seen that many of the above general active attack threats correspond either closely or exactly to those previously described as applicable to the token during transfer between the CDU and ED.

Cryptography is a long-established data security discipline which can be applied to ensure the authenticity and/or secrecy of data. The STS makes use of cryptography to ensure the authenticity of the token transfer process.

At the foundation of this use is a *cipher* referred to as the **standard transfer algorithm** (STA).

Ciphers, keys, encryption and decryption

A cipher is a cryptographic *algorithm* which transforms data so that its meaning is unintelligible, thereby concealing it. Typically the algorithm is used in conjunction with a *cryptographic key* - an algorithm parameter.

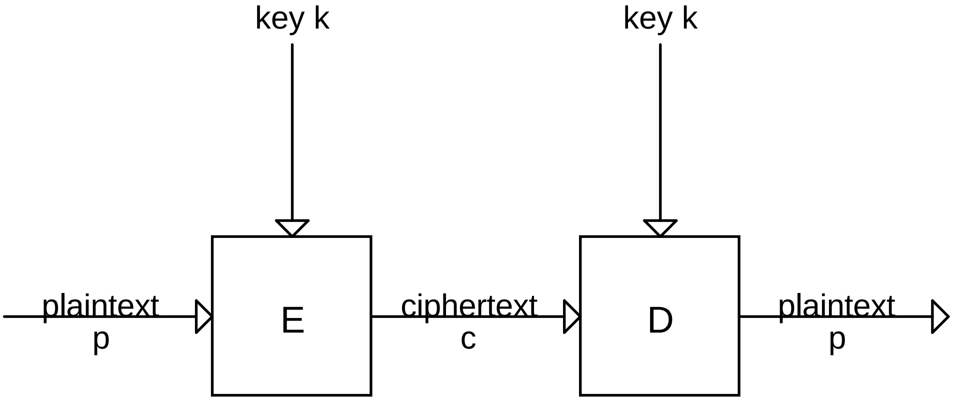


Figure 5

The process consists of the two operations of *encryption* (encipherment) and *decryption* (decipherment). As depicted in figure 5, the two operations can be described as functions of two variables (or for implementation purposes, algorithms with two parameters). The *plaintext* mentioned in the figure is the set of data before encryption. The result of the encryption is the *ciphertext*. The result of applying decryption to the ciphertext is plaintext. In the notation used in figure 2 where *E* and *D* signify encryption and decryption respectively, if *p* is the plaintext, then *c=E(k,p)* is the ciphertext result and the inverse function *p=D(k,c)* expresses decryption of the ciphertext *c* to produce the plaintext *p*. In both functions, the other variable *k* is the key.

The key is an essential feature of a cipher. If the function *c=E(p)* without a key were kept secret, this might serve to conceal the value of *p* but, if the secret of function E is lost, nothing can be done to restore the usefulness of the cipher - an entirely new cipher is needed. Relying on secrecy of the cipher is impractical, since keeping the cipher secret would rely on all those who took part in the design and testing or who wrote programs using the cipher in an application to be trusted indefinitely.

Hence use is made of the key *k*, which is kept secret. If a key is compromised (discovered by an adversary or someone untrustworthy), it can be changed and the cipher can remain in use as is. Secrecy of the function or algorithm as well as the key is a useful security measure but, considering how many people must know it if it is to be usefully applied, secrecy of the function cannot be relied upon by itself - it is the secrecy of the key that matters.

From the perspective of keys, ciphers can be broadly classified as either symmetric ciphers or asymmetric ciphers. Symmetric cipher systems employ a single secret key which is known to both the sender and the receiver of the data - the symmetry is evident in that knowledge of the secret key by both parties A and B allows secret communication from A to B or from B to A. Asymmetric cipher systems employ a dual key system in which the sender and receiver use different but related keys, only one of which need be kept secret. The receiver of the data holds a secret key with which to decrypt, but a different key is used by the sender to encrypt and this can be made public without compromising the system. This is an asymmetric system, providing secret communication in only one direction.

Key management

When encryption is used to make data secure in communications, there must be prior agreement between the communicating parties about all aspects of the procedure. A cipher algorithm, and the method of using it must be agreed. A key must be chosen and made available at both ends of the communication path. Before encrypted data can flow between the two parties, the value of the chosen key must make a similar journey. Keys can be encrypted using other keys but in the end at least one key has to be distributed by some other means. Choosing the key in the first place and making it available only to authorized parties are aspects of *key management*.

After encipherment methods have been decided, key management is the next major task, since the security of the system has then been concentrated in the keys, and is dependent upon their secrecy. In effect, encryption concentrates the risk of discovery on the key in order that the data to be secured can be handled more easily. For this reason, the management of the keys is vital to the security of data encrypted with those keys.

The problem of replay

The process of token encryption described does not completely address the token authentication requirements outlined, because an encrypted token can be recorded by an adversary and later reused as a bogus token, provided this is done during the lifetime of the key. In general as well as in this specific application, it is this possibility of **replay** which complicates authentication.

In general, the solution to the problem of replay is simple in principle - it requires that each data message should be different from all preceding messages using the same key and that the receiver should be able to test the "newness" of each message. Furthermore, the sequence of messages which together form a transaction must be linked in some way so that their sequence can be checked. Protection against replay would be complete if the receiver compared its received messages with all those it had previously received using the same key and rejected messages that were copies.

CONCLUSION

In summary, STS defines:

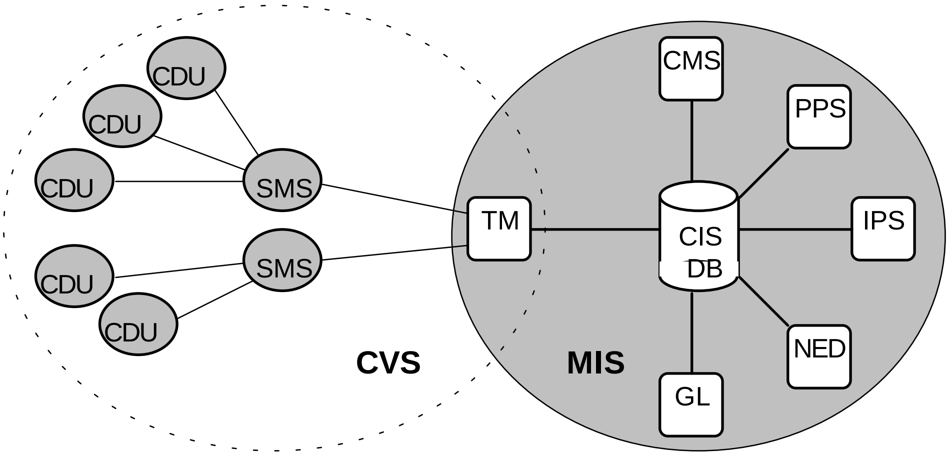
- a set of management and credit functions to be supported by an ED;
- the various data elements required by the CDU to support the implementation of these management and credit functions;
- the format of management and credit token data corresponding to these management and credit functions, as output by CDs, transferred via tokens, and input by EDs;
- the *cryptographic* methods of *encrypting* and *decrypting* this formatted token data so as to ensure its *authenticity* and/or *secrecy* during transfer between CDU and ED;
- the cryptographic methods of *key management* in support of the encryption and decryption of token data;
- the types of *token technology* that can be input by EDs and therefore the token technologies that need to be output by CDs supporting vending to those EDs;
- the method of encoding token data for each type of token technology.

APPENDIX A

Common vending system overview

The system's architecture and implementation of the agent's vending system may take on many and varied forms. Irrespective of this, the STS standards apply to the interface between the CDU and ED. A brief overview of Eskom's CVS is included to provide some background on the interaction between a vending system and the CD.

The CVS consists of multiple groups of *credit dispensers* (CDs) called *credit dispensing units* (CDUs), distributed at various point of sale (POS) locations, with each CDU group concentrated by a *system master station* (SMS). The SMSs are in turn concentrated by a *transaction manager* (TM) on Eskom's *mainframe information system* (MIS), forming a hierarchical system/network architecture.



CDU - Credit Dispensing Unit
CVS - Common Vending System
SMS - System Master Station
TM - Transaction Manager
____ Data Transfer
____ Data Storage

CIS DB - Customer Information System Data Base
CMS - Customer Management System
GL - General Ledger
IPS - Power Billing System
MIS - Mainframe Information System
NED - Nedisys - ED Tracking System

Figure 6 - CVS overview

As depicted in figure 6, various other sub-systems at the MIS support the CVS, but for the purpose of this document, the term CVS incorporates the network of CDUs, SMSs and the TM interfacing them to the MIS.

The hardware and software currently utilised for the CVS entities is depicted in figure 7.

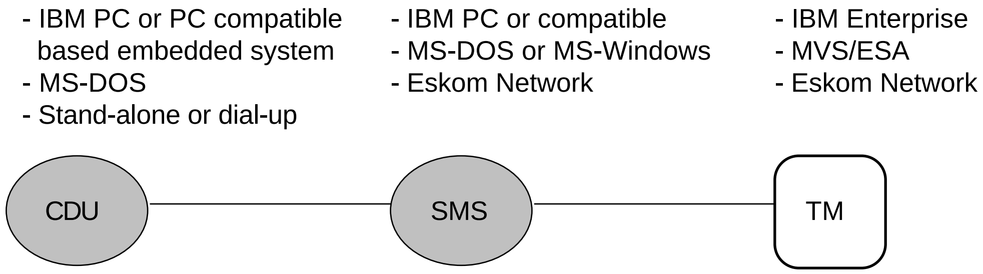


Figure 7 - CVS System Entity Hardware and Software

The CVS provides for the vending of a standard transfer specification (STS) token which enables a purchased amount of electricity for a specific electricity dispenser (ED) to be entered into that ED by the customer, and activate the supply of the corresponding number of units of electricity. The CDU is able to vend STS tokens to customers for EDs designed and manufactured according to the STS - i.e. EDs which support the standard transfer algorithm (STA) and token medias and formats defined by the STS. The CDU also has the capability to interface to a *standard token translator* (STT) to support a manufacturer proprietary token utilising a proprietary algorithm, token format and/or media, thereby ensuring backward compatibility for manufacturer proprietary EDs already installed.

APPENDIX B

STS TROUBLE SHOOTING GUIDE

1 TOKEN CATEGORIES

There are three token categories. These categories are:

- credit transfer tokens,
- dispenser specific management tokens.
- non-dispenser specific management tokens,

The management tokens can be either mandatory or optional. All mandatory tokens must be successfully accepted and processed by an ED. An example is the TEST ALL management token. Optional tokens can, but need not be, accepted and processed by an ED. If an optional token is not supported by the ED, it must indicate that the token has been rejected. Examples of this are the individual test functions.

A token is either dispenser specific or non-dispenser specific. Where a token's use is limited to a particular ED or group of EDs, it is dispenser specific. Where a token can be used at any dispenser, it is non-dispenser specific. Typically, a dispenser specific token is used to alter some state in the meter, eg trip level or reset tamper; and a non-dispenser specific token is used to display items such as key revision number or tamper status.

2 CREDIT TOKENS

Once a credit token has been entered into the ED, and the ED has accepted and processed the token, an indication of this acceptance is given by the ED. In most cases, the number of units transferred id displayed on the LCD, and one or more LEDs may light up on the front panel.

If a credit token is not accepted, the ED will give an indication of this rejection. There are a number of reasons for an ED to reject a token. These are listed below, together with the means to check for reason for rejection.

The text below often refers to information printed on the token. Examples of tokens and the information contained printed on them, for both magnetic card and numeric tokens, are given at the end of the section.

3 REASONS FOR NOT ACCEPTING CREDIT TOKENS

There are a number of reasons for the ED not to accept a credit token. These are :

1. Token physically damaged,
2. Meter number incorrect,
3. Meter key incorrect,
4. Token used,
5. Token old, and
6. ED full

These are described below.

3.1 Token physically damaged (Magnetic card only)

If the token is physically damaged, the meter will not read it at all, and will give no indication of acceptance or rejection of the token.

3.2 Meter number incorrect

If the meter number used to generate the token is incorrect, the token will not be accepted by that meter as the key will be wrong. The meter will give an indication of rejecting the token. In order to check if the meter number is correct, one must compare the meter numbers printed on the front of the ED, embossed on the meter card, and printed on the token on the token. If there are any differences, the correct number is always the one on the actual ED. If the meter number embossed on the plastic meter card is incorrect, it could be either that the wrong card was issued with the meter (with a brand new meter), or else that the card has been swapped with another user.

The first two digits of the meter number denote the manufacturer of the meter. The following table lists the codes currently in use :

CODE	MANUFACTURER
01	AEG Energy Control
02	Budgy
03	Altech
04	Conlog
06	Plessey Tellumat
07	Spescom / EML

For example, if the meter number is 04040900104, the first two digits are 04, so it must be a Conlog meter; and if the meter number is 07816561075 it must be a Spescom / EML meter.

3.3 Meter key incorrect

If the key is incorrect, the meter will not accept the token. The meter will give an indication of rejecting the token. The first reason for the key being incorrect is that the meter number used is incorrect, as discussed above. There are three other reasons for getting an incorrect key, and these are described below.

3.3.1 SGC incorrect

The only way to check if the supply group is correct, is to look at the supply group code printed on the token. This value should be correct for the area in which the meter is installed. If it not correct, it could be either because the meter card has been incorrectly coded, or that the customer record is incorrect on the CDU database.

3.3.2 Tariff index (TI) incorrect

If the TI is incorrect, it will lead to an incorrect key being used for the token. There are two ways to check what TI is being used. Firstly, the TI is printed on the token. Secondly, it can be read out of the ED using a test token, either the general test-all token, or, if supported by the ED, a specific test token to display the TI can be used. These two values must then be compared. If they are different, this is probably the reason for the ED not accepting the token.

3.3.3 Key revision number (KRN) incorrect

If the KRN is incorrect, it will lead to an incorrect key being used for the token. There are two ways to check what KRN is being used. Firstly, the KRN is printed on the token. Secondly, it can be read out of the ED using a test token, either the general test-all token, or, if supported by the ED, a specific test token to display the KRN can be used. These two values must then be compared. If they are different, this is probably the reason for the ED not accepting the token.

3.4 Token used

A security feature built into the STS is that no credit token can be used more than once. This is achieved by having an identifier built into the token. These identifiers are stored in a table in the ED, and the identifier of a new token is compared to the table, and if it has already been entered into the ED, the token will be rejected. The ED will give a notification that the token is used. In the case of certain magnetic card ED, the token is physically marked, ie it has a hole punched through it, and will not be read by the ED at all.

3.5 Token old

Due to the nature of the token identifier, an STS token has an effective shelf life of approximately three months. If a token that is older than three months is entered, the ED may reject that token, and give an indication on the front panel that the token is old.

3.6 ED full

An ED has a maximum amount of credit that it can store. If the number of units on the token will cause the ED credit to exceed this maximum value, the token will be rejected. The token may be entered at a later date when the level of credit in the ED has reduced enough to accept this token. The ED will give an indication that it is full.

4 DISPENSER SPECIFIC MANAGEMENT TOKENS

The following dispenser specific management tokens are available with STS :

- Set maximum power load,
- Clear credit,
- Clear tamper,
- Set ED key.

These tokens are very similar to credit tokens, as they are encrypted, can only be used once, and alter the state of the meter. In the case of a dispenser specific management token not being accepted, the same trouble shooting principles as for credit tokens apply, with the exception of the ED full condition.

4.1 Set ED key token

In the case of the SET ED KEY function, a pair of tokens will be issued. These two tokens may be entered in any order. However, if the is a long delay between entering the two tokens, the ED may timeout and forget the first key change token entered. This tokmeout varies from ED to ED, and is not implemented on all EDs.

When the first token is issued, the ED accepts it, but performs no action on it. Only after accepting the second token will the ED actually perform the key change.

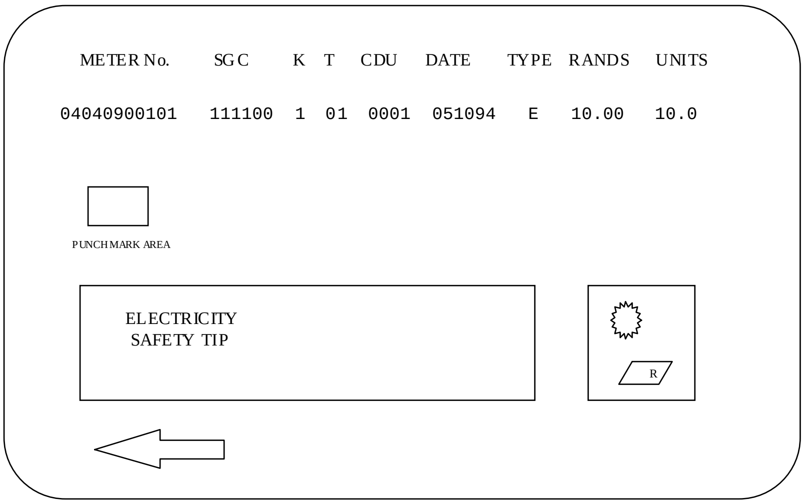
These key change tokens are encrypted in the same way as credit tokens, thus the trouble shooting procedure for non-acceptance is the same as for credit tokens.

5 NON-DISPENSER SPECIFIC MANAGEMENT TOKENS

Non-dispenser specific management tokens are different from the other two types of token in that they are not encrypted, ie they can work in any ED, and they can be used many times. Thus the only reason for not accepting one of these tokens is that the token is physically damaged in the case of a magnetic card token, or that the number has been incorrectly keyed into the ED.

6 STS TOKENS

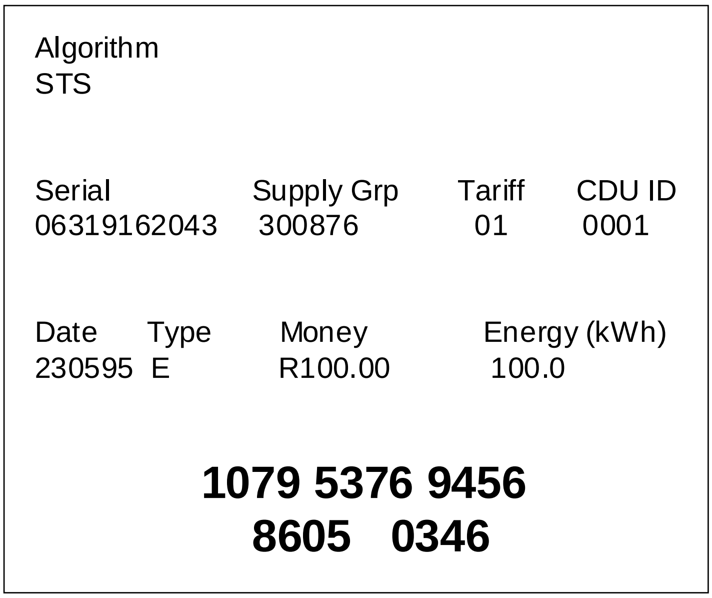
6.1 STS MAGNETIC CARD TOKEN


METER No. SGC K T CDU DATE TYPE RANDS UNITS
04040900101 111100 1 01 0001 051094 E 10.00 10.0
PUNCHMARK AREA
ELECTRICITY
SAFETY TIP
R

The following information is printed on the magnetic card :

TOKEN FIELD	DESCRIPTION
METER No.	ED serial number
SGC	Supply group code
K	Key revision number
T	Tariff index
CDU	CDU ID from where token was purchased
DATE	Date of issue of the token
TYPE	Type of token
RANDS	Monetary value of units purchased
UNITS	Unit amount purchased

6.2 STS NUMERIC TOKEN



```
Algorithm
STS

Serial          Supply Grp    Tariff   CDU ID
06319162043     300876        01       0001

Date     Type     Money        Energy (kWh)
230595   E        R100.00      100.0

          1079 5376 9456
            8605   0346
```

The following information is printed on the numeric token :

TOKEN FIELD	DESCRIPTION
Serial	ED serial number
Supply Grp	Supply group code
	Key revision number
Tariff	Tariff index
CDU ID	CDU ID from where token was purchased
Date	Date of issue of the token
Type	Type of token
Money	Monetary value of units purchased
Energy (kWh)	Unit amount purchased