TID ROLLOVER CHECKLIST AND TIMELINE

STS ASSOCIATION

STS1800-3

Edition 1.0 Sept 2015

Contents

1. Introduction

The Token Identifier is a 24 bit field, contained in STS compliant tokens, that identifies the date and time of the token generation. It is used to determine if a token has already been used in a payment meter. The TID represents the minutes elapsed since the 1st January 1993. The incrementing of the 24 bit field means that at some point in time, the TID value will roll over to a zero value.

All STS prepayment meters will be affected by TID roll over on the 24/11/2024. Any tokens generated after this date and utilizing the 24bit TID will be rejected by the meters as being old tokens as the TID value embedded in the token will have reset back to 0.

In order to overcome this problem all meters will require key change tokens with the roll over bit set. In addition to this, the base date of 01/01/1993 will be required to be changed to a later date. This process will force the meters to reset the TID stack to 0. To avoid previously played tokens from being accepted by the meter due to the TID stack reset, the key change process must introduce into the meter, a new decoder key.

A process is therefore required to allow for the management of this change with the least impact to the Utilities and equipment suppliers.

2. Benefits of a TID rollover

The STS system has been stable and successful over the past 20 years. Technology however, moves on. The time has come for the STS system to include positive changes that will ensure that the system continues t operate the way it has since its inception.

Some of the benefits of this process are:

1. Significantly stronger algorithms for vending key creation and protection - the new system will use up to 192 bit encryption and state-of-the -art algorithms.

2. Key expiration - the new system will allow for a vending key to be expired after a certain time (chosen by the SGC owner). This ensures that even if a vending key has been compromised, the key will expire after a certain time. This will significantly reduce the risks associated if a vending system or security module is stolen.

3. The longevity of the STS system is guaranteed.

4. All meters that have been using tokens purchased from un-authorized vendors will no longer be able to purchase from those vendors.

3. Process Overview

The process that should be followed to ensure that a smooth and successful the TID Rollover is carried out to all meters is outlined in the sections below.

3.1 Update (develop) security module-OK

Security modules - vending and manufacturing - to be updated to cater for key-change with rollover bit set on selection of a new base date. Deployment of the security module can only commence after the deployment of the updated KMC.

3.2 Update KMC

KMC to be updated to generate keys dependent on base date. This new KMC will allow coding of the upgraded security module. At the same time, introduce stronger algorithms to protect the vending keys from attack. This is the first step in the chain.

3.3 Update Meters

Meters to be manufactured with new base date of 2014 by selecting a vending key with a base date of 2014 - no further changes required to manufactured meters. This will require updating of manufacturing security modules, as well as the manufacturing processes to cater for multiple base dates for the duration of the changeover period.

3.4 Update vending systems

Vending systems to be updated to cater for multiple base date functionality in the security module. This will include the handling of a new key-load file specification as contained in STS600-4-2.

3.5 STSA test houses to certify all new vending systems and SM

Accredited test houses to certify all updated vending systems and security modules. STSA to issue certificates.

3.6 Meter key-change program

Meter key-change program for the updating of all meter keys in the field. Utilities and sub-vendors to put together a program to handle all their meters by SGC and if necessary, by meter groups for large SGC's.

4. Action Plan

4.1. STSA

The function of the STSA in this program is to ensure that all STS users are made aware of this program, either via direct member/utility contact, or through their membership. The STSA will also manage the overall project timeline, but not the implementation of the project.

The STSA will further manage the rollout of the new KMC and updated security module.

4.1.1 Checklist of actions required

- Development of this document
- Communications to all its members regarding the rollout plan
- General assistance in the handling of rollover queries
- Development of CTS tests for the new SM and KMC
- Manage the updated KMC project
- It may be necessary to update the IE62055-41 specification to allow for two vending keys to be resident in the SM for key-change as well as the generation of vending tokens. This is to allow smaller groups of meters within an SGC to be key-changed instead of an entire SGC at the same time.

4.2 Secure module suppliers

Secure module suppliers will be required to upgrade security modules to cater for the rollover bit as well as the handling of multiple base dates. The SM supplier should also be in a position to communicate with their customers to inform them of the requirement to upgrade their SM's.

4.2.1 Checklist of actions required

- Upgrade SM to cater for rollover bit and multiple base dates
- Test SM - initialization, key-loading, and new firmware functionality to STS600-4-2 specification
- Certify SM to CTS spec for STS600-4-2 (STS531-8-2)
- Field test SM - code at KMC and test tokens with live keys
- Deploy SM to the field once KMC deployed and vending systems have beenupdated.

4.3 KMC Suppliers

KMC suppliers will be required to manage the upgrade to the existing KMC, and rollout the new KMC supporting multiple base date functionality. A migration of data will be required from the old to the new KMC.

4.3.1 Checklist of actions required

- Upgrade KMC to cater for multiple base dates as per STS600-4-2
- Migrate all data from current KMC to new KMC
- Test SM initialization and key-loading to new KLF specification
- User acceptance testing of KMC
- Field test KMC
- Get STSA approval for KMC
- Deploy the new KMC

4.4 Key management centre

The Key Management Centre will be required to generate a list of all SGC owners so that they can be contacted. In addition to this, they will need to be fully trained in the use of the upgraded KMC.

4.4.1 Checklist of actions required

- New KMC training
- Field test - code TSM250 SM's. Generate key with rollover bit set, test on live meter
- Generation of a list of all SGC's and security modules for communications strategy
- Code all new SM's supporting rollover bit (STS6) from manufacturers and utilities
- Update their processes for the new SM and KMC since these will differ from the current system.

4.5 Meter manufacturers

Meter manufacturers will have to change their production processes in order to cater for the new manufacturing PAM modules. They will also be required to start manufacture of meters on the 2014 base date as per the timing plan.

4.5.1 Checklist of actions required

- Update manufacturing modules
- Check rollover bit functionality in meters
- Change production processes to cater for multiple base dates
- Manufacture meters with new base dates

4.6 Vending system manufacturers

Vending system manufacturers will be required to update all the vending software to cater for the new API and key-load files and rules. They will also be required to contact all their customers to arrange for software upgrades to be performed in the field. In addition to this, contact details should be made available for all sub-vendors that they have business with so that they may be informed of the TID rollover.

4.6.1 Checklist of actions required

- Update software to cater for new KLF specification
- Update software to handle multiple base dates
- Certify software to CTS test specs
- Upgrade customer vending software in the field
- Get contact details of all sub-vendors that use their vending systems

4.7 Utilities

Utilities will be responsible for the rollout plan of the key-changes to the new base date. This program must be set up by the utilities themselves based on the timing requirements of the project timelines. This part of the project is naturally the most important and difficult of the entire project and must be though out thoroughly before implementation.

4.7.1 Checklist of actions required

- Upgrade all SM's to STS6 functionality
- Select SGC's to do key-changes
- Decide on key-change process (manual or automatic)
- Inform all users and regions of the program
- Generate a program for KCT's - whether by SGC of smaller groups of meters

- Start the program on a pilot site
- Roll out to all SGC's
- Ensure that the entire program is completed at least one year before the TID rollover date of 2024.

4.8 Sub-vendors

All sub-vendors need to be contacted via KMC and manufacturer lists and contacts. They will not be aware of the TID rollover since most of them are not members of the STSA. The STSA should begin this task as soon as possible.

4.8.1 Checklist of actions required

- Upgrade SM's to STS6 functionality
- Generate key-changes with rollover for all meters
- Carry out the key-changes to all meters

4.9 Tools/specifications requiring updates

4.9.1 VSM

- Update VSM to cater for new base dates
- Allow import of KLF using VSM allocated keys (to be discussed with Prism)
- Update VSM to handle new KLF specification

4.9.2 Nedysis file specification

The Nedysis file system is not used by all utilities, but needs to be updated for those that do use it. The update requires that a base date field be added to specify which base date a meter is allocated to.

4.10 Accredited STSA test houses

Test houses will be required to test all vending systems that have been modified to cater for the new SM's. Security modules will also require accreditation.

4.10.1 Checklist of actions required

- Study the new test documents for approval of vending systems and SM's
- Allocate time to testing for compliance

5. Overall project implementation timeline

Year	2016				2017				2018		2023	
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1-Q4		Q4	
SM Manufacturers												
SM update to STS6												
SM field test												
SM certification												
SM Deployment												
KMC manufacturers												
KMC update												
KMC data migration												
KMC UAT (+ field trial)												
KMC training												
KMC approval (STSA)												
KMC Deployment												
Meter manufacturers												
Update production processes												
Start meter manufacture to new base dates												
Vending Software Manufacturers												
Upgrade all SM's to STS6												
Upgrade vending software												
Software accreditation to CTS												
Update customer software in the field												
Utilities												
Update all field SM's												
Communications program rollout												
Select SGC's												
Run pilot												
Generate program												
Rollout to all areas												
Sub -vendors												
Contact all sub - vendors												
Upgrade SM to STS6 with new base dates												
Perform key - changes												
Field Key Changes												
Complete all key - changes												

Further information about the Standard Transfer Specification and the STS Association may be found on the Association's website www.sts.org.za or by contacting the Secretariat.

Secretariat: Mr. Jean Venter / Adrie da Silva

P.O. Box 868, Ferndale, 2160, Johannesburg, South Africa.
Tel: +2711 061 5000
sts@vdw.co.za