STS Association

STS1800-3

Edition 1.2 Oct 2018

TID Rollover Checklist and Timeline

Contents

Revision History

Revision	Clause	Date	Change details from previous Edition
1.0	General	Sept 2015	Initial revision
1.1	General	October 2018	Updated document to reflect current status, various editorial changes, removed hanging clauses.
1.2	general	October2018	Corrected broken links

1 Definitions

HSM: Hardware Security Module

KLF: Keyload File

SGC: Supply Group Code

SM: Security module

STSA: STS Association

VSM: Virtual Security Module

CTS: Conformance Test Specifications

2 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 number of minutes elapsed since the base date of 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 24-bit TID, calculated on base date 1993, will be rejected by the meters as being old tokens as the TID value encoded in the token will have reset back to 0.

In order to overcome the TID rollover occurrence, 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 base date of 01/01/2014. This process will force the meters to reset the TID stack memory to 0. To avoid previously used tokens from being accepted by the meter due to the TID stack reset, the key change process changes the meter key at the same time.

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

3 Benefits of a TID rollover and STS Edition 2

The STS Edition 1 Specifications have been used successfully for more than 25 years, and with the recent launch of STS Edition 2 specifications, significant benefits for the industry can be realised, these being:

1. Enhanced algorithms for vending key creation and protection - the new system will use up to 192 bit encryption and state-of-the -art algorithms approved by NIST for use at least up to 2045.

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 with the theft of standalone vending systems or security modules.
3. The longevity of the STS system is guaranteed.
4. All STS prepayment meters that have been using tokens purchased from un-authorised vendors will reject these tokens after the TID rollover key changes have been performed.

4 Process Overview

4.1 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.

4.2 Update Key Management Centre (KMC)

The KMC has been updated to support the upgraded security levels in compliance with STS 600-4-2 and also to support the updated security modules (see below). The KMC still supports the legacy key management protocols.

4.3 Update security module

Vending and manufacturing security modules have been upgraded to support the upgraded security levels and the generation of TID rollover key change tokens. The upgraded security modules have a new API (known as STS6), that requires additional vending and manufacturing software changes (see below).

The upgrade path of the various security module models is given in the table below.

TSM210	Replace with TSM250
TSM220	Replace with TSM250
TSM250	Send to Prism for firmware upgrade to STS6
TSM410	Replace with TSM500
TSM500	Send to Prism for firmware upgrade to STS6

Prism's contact details are as follows:

Att: Shawn O'Neil

Email: Shawn O'Neill shawno@zazooltd.com

Tel: +27 (0)31 267 5500

4.4 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 defined in STS600-4-2, and conformance

to the STS600-8-6 HSM protocol All vending systems are to be re-certified to ensure compliance with these new requirements. Note that after June 2019, all vending systems must be compliant to the new requirements of the STS Edition 2 suite of standards (See Appendix A).

4.5 Update Meter Manufacturing Process

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

Note that utilities can only utilise meters manufactured on base date 2014 after their vending software has been updated and should only do so upon specific request from the utilities.

The meter certification test facility could not test for TID rollover functionality prior to 2014, so there is a small risk that some of those meters may not correctly support the TID rollover key change. Utilities and meter manufacturers must select samples of these meters and resubmit them for testing. The STS Association will do the test free of charge. Those meters that do not comply must then be replaced in the field. A list of meters/suppliers falling into this category is available from the STS Association.

4.6 STSA Test Facilities

Accredited STSA test facilities are now able to certify all updated vending systems and security modules. These will be issued with new certificates and all prior compliance certificates will be revoked after June 2019.

4.7 Meter key-change program

Utilities and sub-vendors must develop a program to manage the TID rollover key changes to all installed meters operating on base date 1993. Those meters already operating on base date 2014 do not need their meter keys changed.

In certain cases this program will be a huge undertaking and utilities are thus advised to start as soon as possible.

There are two possible options to follow:

1. The end-customer may be issued with the key change token pair at the time when he next purchases credit at a vending station. He then enters the token pair into his meter himself before he enters his newly purchased credit token.

2. A dedicated field-service team may be used to visit each meter and then enter the key change token pair.

The STS Association is available to assist and advise utilities and sub-vendors on the appropriate approach to take.

5 Action Plan

5.1 STS Association

5.1.1 General

The STS Association (STSA) is putting in place the necessary infrastructure and has launched a campaign to make all STS users aware of the TID rollover requirements and to assist and advise users in the execution of the TID rollover key change program.

5.1.2 Checklist of actions required

- STSA to communicate to all its members regarding the rollout plan - this process is under way;
- General assistance from the STSA technical support in respect to rollover queries;
- Development of CTS tests for the new SM and KMC - this has been completed;
- Manage the updated KMC project - this has been completed.

5.2 Secure module suppliers

5.2.1 General

Upgrading of Secure Modules (SMs) to cater for the rollover bit as well as the handling of multiple base dates has been completed. It is the responsibility of the SM supplier to communicate with their customers to inform them of the requirement to upgrade their SMs.

All SMs that do not support the STS6 protocol must be upgraded, this includes the TSM210, TSM250, TSM410 and TSM500 models.

5.2.2 Checklist of actions required

- Upgrade SM to cater for rollover bit and multiple base dates - this has been completed;
- Test SM - initialization, key-loading, and new firmware functionality to STS600-4-2 specification - this has been completed;
- Certify SM to CTS spec for STS600-4-2 (STS531-8-2) - this has been completed;
- Field test SM - code at KMC and test tokens with live keys - this has been completed;
- Deploy upgraded SM to the field - this has started.

5.3 Key Management Centre (KMC) suppliers

Upgrade to the existing KMC and rollout the new KMC supporting multiple base date functionality has been completed.

5.4 Key Management Centre

5.4.1 Overview

The Key Management Centre has been upgraded in compliance with STS 600-4-2 and is fully operational regarding support for the TID rollover program.

5.4.2 Checklist of actions required

- Issue new vending keys in the new key load file format to upgraded vending and meter manufacturer systems when so requested and are ready to receive them;
- Maintain support for legacy key load files until all TID rollover key change programs have been completed.

5.5 Meter manufacturers

5.5.1 Overview

Meter manufacturers must update their production processes in order to cater for the new manufacturing security modules, and to enable them to manufacture meters on either base date as specified and so requested by their customers.

5.5.2 Checklist of actions required

- Update manufacturing modules - this has started;
- Check rollover bit functionality in meters - this has started;
- Change production processes to cater for multiple base dates - this has started;
- Manufacture meters with new base date of 2014 when requested to do so by their customers.

5.6 Vending system manufacturers

5.6.1 Overview

Vending system manufacturers are required to update all the operational vending software to cater for the new SM 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.

5.6.2 Checklist of actions required

- Update software to cater for new Key Load File (KLF) specification - this has started;
- Update software to handle multiple base dates - this has started;
- Certify software to CTS test specs - this has started;
- Upgrade customer vending software in the field - this has started;
- Get contact details of all sub-vendors that use their vending systems and communicate these to the STS Association.

5.7 Utilities

5.7.1 Overview

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

5.7.2 Checklist of actions required

- Request the vending system supplier to upgrade the vending system as per 5.6 above;

- In the case where the utility had developed their own vending system, the utility must do the upgrade as per 5.6 above;
- Divide the installed base of meters into smaller manageable groups for processing one group at a time;
- Decide on key-change program option as per 4.7 above;
- Compile a program for the entire key change operation;
- Inform all role players (especially the end-customers) and regions of the program details;
- Start the program on a pilot site to test the processes;
- Roll out to other meter groups;
- Ensure that the entire program is completed at least one year before the TID rollover date of 2024;
- As soon as the vending system has been upgraded, new orders for meters should instruct their meter vendor to manufacture those meters on base date 2014.

5.8 Sub-vendors

5.8.1 Overview

Sub-vendors are responsible for the rollout plan of the key-changes to the new base date on meters that are under their control. This program must be set up by the sub-vendors themselves, based on the timing requirements of the program timelines. This part of the program is naturally the most important and difficult of the entire program and must be thought out thoroughly before implementation.

5.8.2 Checklist of actions required

- Request the vending system supplier to upgrade the vending system as per 5.6 above;
- Divide the installed base of meters into smaller manageable groups for processing one group at a time;
- Decide on the key-change program option as per 4.7 above;
- Compile a program for the entire key change operation;
- Inform all role players (especially the end-customers) and regions of the program details;
- Start the program on a pilot site to test the processes;
- Roll out to other meter groups;
- Ensure that the entire program is completed at least one year before the TID rollover date of 2024;
- As soon as the vending system has been upgraded, new orders for meters should instruct their meter vendor to manufacture those meters on base date 2014.

5.9 Tools/specifications requiring updates

5.9.1 Virtual Secure Module (VSM)

- The update of the VSM to cater for new base dates has been completed;
- Allow import of KLF using VSM allocated keys;

- Update VSM to handle new KLF specification;
- Release updated VSM for use.

5.9.2 Nedisys file specification

The specification (ST_240-76627071_Prepaid Meter upload standard Rev4) may be obtained from Eskom at http://www.prepayment.eskom.co.za.

6 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												

Note: Items in blue are completed. Shaded items started but not completed.

7 Appendix A (informative)

The STS Edition 2 document suite comprises the following documents:

IEC62055-41 Ed3 2018	Electricity metering – Payment systems – Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems
STS101-1	Physical Layer Mechanical and Electrical Interface for Virtual Token Carriers
STS101-2	Physical Layer Protocol for a two-way virtual token carrier for remote connection over DLMS/COSEM
STS201-1	Meter function object: RegisterTable for payment meters
STS202-4	Physical layer protocol for a two-way virtual token carrier for direct local connection
STS202-5	Class 2 token extensions
STS202-6	Additional requirements for vending systems
STS203-1	Method for default Payment Meter values for conformance testing
STS531-0 (ED 1.9)	COMPLIANCE TEST SPECIFICATION - Quality Plan
STS531-1-0-02 (ED 1.9)	Entity Type A - POSToTokenCarrierInterface application layer protocol for POS devices supporting DKGA=02 and EA=07, and optionally: DKGA=04 and EA=07
STS531-1-0-04 (ED 1.9)	Entity Type A - POSToTokenCarrierInterface application layer protocol for POS devices supporting DKGA=04 and EA=11, and optionally: DKGA=04 and EA=07
STS531-1-1-04 (ED 1.9)	Entity Type A - POSToTokenCarrierInterface application layer protocol for POS devices supporting DKGA=04 and EA=07
STS531-2-1 (ED 1.9)	Entity Type B - POSToTokenCarrierInterface physical layer protocol for TCT = 01 and TCT = 02
STS531-3 (ED 1.9)	Entity Type C – Token Carrier: Token Carrier for TCT = 01 and TCT=02
STS531-4 (ED 1.9)	Entity Type D: Token Carrier to Meter Interface Physical Layer Protocol for TCT = 01 and TCT = 02
STS531-5-0 (ED 1.9)	Entity Type E - TokenCarriertoMeterInterface Application Layer Protocol for TCT = 01 and TCT=02
STS531-6-1-07 (ED 1.9)	Entity Type F – MeterApplicationProcess for TCT = 01 and TCT = 02, Using EA=07
STS531-6-1-11 (ED 1.9)	Entity Type F – MeterApplicationProcess for TCT = 01 and TCT = 02, Using EA=11
STS531-8-1 (ED 1.9)	Entity Type H – POS to Security Module Interface
STS531-8-2 (ED 1.9)	Entity Type H – POS to Security Module Interface Supporting DKGA=01, DKGA=02, DKGA=04, EA=07, and EA=11
STS531-10-02 (ED 1.9)	Entity Type H1 - SecurityModuleToPOSInterface adaptation

	layer protocol for POS devices supporting DKGA=02 and EA=07, and optionally: DKGA=04 and EA=07
STS531-10-04 (ED 1.9)	Entity Type H1 - SecurityModuleToPOSInterface adaptation layer protocol for POS devices supporting DKGA=04 and EA=11, and optionally: DKGA=04 and EA=07
STS600-4-2	Key Management System
STS600-8-1	Legacy Security Module API for STS03V
STS600-8-2	Legacy Security Module API for STS03M
STS600-8-3	Legacy Security Module API for STS04A
STS600-8-4	Legacy Security Module API for STS05V
STS600-8-5	Legacy Security Module API for STS05M
STS600-8-6	Security Module API for STS6
STS600-15	Key Management Systems forms
STS1800-7	Manufacturing guidelines