Standard Transfer Specification Association
4 Karen Street, Bryanston West
Johannesburg, South Africa
Telephone: +27 11 061 5000
e-mail: sts@vdw.co.za
web: www.sts.org.za

STS ASSOCIATION

STS TID rollover and security upgrade

FREQUENTLY ASKED QUESTIONS

11/08/2018 Draft 1.02

1 Introduction

Each token is encoded with a unique Token Identifier (TID), which has a limited range and will run out (roll over) on 24 November 2024. After this date all STS compliant meters will stop accepting credit tokens, unless an intervention takes place, which means that all these meters need to receive the TID Rollover Key Change with new base date before this date.

The STS Association has been in operation now for the past 25 years without any known compromise of its security level and vending keys. This risk is ever increasing due to the natural evolution of computing power, which roughly doubles every 18 months. Extending the current vending and meter keys' lifetime beyond 2024 would be increasing this risk to unacceptably high levels and exposure to the industry.

In mitigation of this risk, the STS Association has thus upgraded the security level of the STS, which entails the publication of STS600-4-2 and IEC62055-41 Ed3 standards. It is therefore a mandatory requirement for all STS systems and products to comply with these standards and specifications before 24 November 2024.

The current STS keys and TID range are linked to a base date of 1993. When the security upgrade and the TID key changes are done, the new keys and the new TID range are linked to a base date of 2014, thus pushing out their "useful life" date to 2045.

The security upgrade and the TID roll over key change take place in the same operation.

The following frequently asked questions attempt to provide STS users with guidelines and insight on how to deal with the above-mentioned issues.

2 What is the significance of the year 2024?

Two major issues need to be addressed before 24 November 2024.

1) The current STS security level of the Secure Module has to be upgraded in compliance with STS600-4-2 as approved by the National Institute of Standards and Technology (NIST).
2) The TokenID (TID) will run out of range on 24 November 2024, which requires that all meters need to receive the TID key Change Tokens before that date, else the meters will stop accepting credit tokens.

3 Why does the security level of the STS need to be upgraded?

The National Institute of Standards and Technology (NIST) is the global reference for cyber security and In 2005 NIST deprecated 56-bit cryptographic keys and algorithms due to the increased risk of compromise by brute force attack.

The STSA upgraded the STS security levels to 160-bit vending keys (now published as STS600-4-2 and IEC 62055-41 Ed3) and is approved by NIST up to 2045.

4 What is STS Edition 2?

STS Edition 2 is a general term used to refer to the latest suite of STS specifications and IEC standards, which includes the security upgrades as specified in STS600-4-2 and IEC 62055-41 Ed3. The relevant STS specifications are available on the STSA website and the IEC standard is available on the IEC web-store https://webstore.iec.ch.

All STS products (old and new) have to comply with STS Edition 2 before 24 November 2024.

5 Why do I have to upgrade to STS Edition 2?

Only STS Edition 2 compliant vending systems are able to generate the special key change tokens for all meters required before the TID rollover event on 24 November 2024.

The STSA mandates that the migration from legacy STS Edition 1 to STS Edition 2 takes place between now and 2024 in order to mitigate the increasing security risk of vending key compromise.

The STS Key Management Centre (KMC) has been upgraded and now complies fully with the requirements of STS Edition 2 and will therefore only support legacy STS products up to 2024.

Secure modules complying with legacy STS Edition 1 specifications, will no longer be supported after 2024.

Product certification services for vending systems with legacy STS Edition 1 certifications, will no longer be supported after June 2019, at which point all old certificates will be revoked.

6 What happens if I don’t upgrade to STS Edition 2?

STS Edition 2 upgrade is required in order to perform the TID rollover key change required before 24 November 2024.

Support for all legacy STS Edition 1 products and services will cease after 2024.

Certificates for vending systems certified to legacy STS Edition 1 specifications will be revoked after June 2019.

7 What does the upgrade to STS Edition 2 entail?

All vending systems’ software must be upgraded and then be re-certified.

All secure modules’ firmware must be upgraded to the certified version STS6 by the secure module supplier. Please contact your secure module supplier to check if your security module is able to receive a firmware update.

8 What is STS6?

This is the firmware version residing on the secure module that supports STS Edition 2.

9 Do I have to upgrade my installed meter base?

Since inception of the STS, all meters have had to comply with the TID rollover key change requirement. However, this functionality could only be tested since February 2014 when the required test tools became available.

There is an uncertainty about meters certified before February 2014, so these meters need to be re-tested for TID rollover key change functionality. No action is required for meters certified after this date.

For installed meters certified before February 2014, one sample meter needs to be taken from the field and sent to the STSA test facility for re-certification of the TID rollover key change function. One sample of each meter type, model and firmware version needs to be submitted. The testing fee will be paid by the STSA, but the sender has to pay for transportation cost of the samples to and from the test house.

In the case where the sample meter fails the TID rollover key change test, all meters of that particular type, model and firmware version need to be replaced prior to the TID rollover key change event.

The utility should have recourse to the supplier of the failed meter type on the grounds that the TID rollover key change function has been a requirement since inception of STS.

10 How do I upgrade my vending system?

Negotiate with your vending system supplier to upgrade the software and have it re-certified.

An upgraded secure module is also required to support the upgraded vending system software.

11 How do I upgrade my secure module?

Negotiate with your secure module supplier to upgrade the firmware or to replace the hardware where this may be appropriate.

Prism TSM210 modules cannot be upgraded, so these need to be replaced with Prism TSM250 modules.

Prism TSM250 and TSM500 modules can be upgraded.

Prism TSM420 modules cannot be upgraded and need to be replaced by TSM500 modules.

Note that the vending system software also needs to be upgraded at the same time.

12 What about product certification?

All STS products have to comply with STS Edition 2 before 24 November 2024, thereafter, certification services of all legacy STS products will cease..

All vending systems must comply with STS Edition 2 before July 2019, after which certification services for vending systems supporting only legacy STS will cease.

Self certification is subject to the rules specified in clause 5.6 of STS 2100-3.

13 What is a TokenID (TID)?

A TID is a token identification code used to uniquely identify each token that is generated.

When a meter accepts a token, it stores the TID in order to prevent the same token of being accepted more than once.

At the time of creation of the token, the TID is calculated as the number of minutes that have elapsed since a given base date.

14 What is TokenID (TID) rollover?

The TID is calculated from a given base date and has a life span of 31.9 years, after which the meter will not accept new tokens.

At the end of its life the TID memory in the meter has to be reset (also known as TID rollover) and the meter key has to be changed to prevent old tokens from being used again.

Existing vending keys are linked to the 1993 base date and a key revision of 1. For this base date the TID reaches its end of life on 24 November 2024.

STS Edition 2 vending keys are linked to a 2014 base date and a new key revision. For this base date the TID reaches its end of life in 2045.

15 When can I start the TID rollover program?

Do not underestimate the magnitude of this operation, so start as soon as possible. There is only a relatively short time left to the 2024 deadline.

Note that the vending system first needs to be upgraded to STS Edition 2.

16 How do I prepare for TID rollover?

Upgrade the vending system software and secure modules to STS Edition 2.

Select sample meters certified before February 2014 and get them re-tested. Replace those meters that are non compliant.

Join the STS user group discussions on the website and learn from the experience of others who are engaged in a similar program.

17 How do I execute the TID rollover key change program?

Establish a project team to plan the operation well in advance and involve your meter suppliers and vending system suppliers.

The purpose of the project should not be communicated to vendors and consumers as this may alert and cause existing fraudulent activities (like ghost vending or meter tampering) to take evasive action ahead of time.

Demarcate meters into smaller groups and do a key change on one group at a time so that the installed base is done systematically under well controlled conditions.

Set up a first-line of support help desk to deal with issues coming from the field and a second-line technical support team to deal with exceptions.

OPTION 1 (most cost effective)

Issue key change tokens to consumers when they purchase credit and instruct them in clear and simple terms to enter the two key change tokens before entering the newly purchased credit token.

Inform them that the newly purchased credit token will only be accepted by the meter if the two key change tokens are entered first. Consider numbering the tokens in the sequence they have to be entered.

Deal with exceptions via the first-line help desk and provide a second-line of technical support to resolve difficult issues.

OPTION 2 (least cost effective)

Issue key change tokens to a dedicated team of technical staff who then visit the meter to enter the tokens themselves.

Deal with exceptions via the first-line help desk and provide a second-line of technical support to resolve difficult issues.

This option provides a good opportunity to do a meter audit and to restore tampered meters at the same time.

18 What support will the STS Association provide regarding TID rollover?

The STS Association has established a task team to provide guidance and support to STS users during the TID rollover key change program.

An STS user forum website is being established where users can participate in discussions and receive guidance from the STSA and other users.

The STS Association will pay for the cost of re-testing sample meters that were certified before February 2014, but the cost of transportation to and from the test house has to be paid by the sender.