STS ASSOCIATION

Simple ▸ Trusted ▸ Secure

TID ROLLOVER PRESENTATION TO ERASA

Token ID Rollover Event in 2024

WHAT IS THE TID ?

- A unique token identifier (TID) is calculated and coded into the token every time a token is created at the POS
- The TID is currently calculated as the number of minutes that have elapsed since a base date of 1993
- The meter records the TID when the token is entered into the meter - this prevents token replay

LIMITATIONS OF THE TID

- The TID has a limited range of 31.9 years
- In November 2024 the TID will reset (roll over) to zero
- Any new tokens after this date will not be accepted by the meter as the meter will consider these as being “OLD”
- The remedy is to clear the meter’s memory of previously accepted TIDs and to change the meter’s cryptographic key at the same time in order to prevent token replay

TID SIZE TRADE-OFF

- Why was the TID not designed to last longer than 31.9 years?
- The token string would be much longer than 20 digits
  - Impractical for consumer entry on keypad
- It is normal practice to upgrade the cryptographic strength at least every 30 years
- It is thus a good compromise to converge the timing of these two elements into one operation

TID ROLLOVER KEY CHANGE

- The current TID is calculated from base date 1993
- A new base date of 2014 has been introduced and is associated with a new vending key revision with increased cryptographic strength that will be good for use up to 2045
- After the TID rollover key change, the new TID will be calculated from the 2014 base date and will have a lifespan up to 2045
- **Utilities are urged to start the process as soon as possible**

STS600-4-2 upgrade

- The STS Key Management Centre has been upgraded to STS600-4-2 operations with legacy support up to 2024
- Hardware Secure Modules are now available with STS600-4-2 certification
  - Existing TSM500i and TSM250 secure modules can be firmware upgraded to STS600-4-2
- Key load files have been upgraded to STS600-4-2
  - Legacy key load files are still supported for existing secure modules and vending keys up to 2024

SECURITY FEATURES in STS Edition 2

- New security features have been included to protect the SGC owner.
- These features are managed between the SGC owner and KMC, and enforced by the security module.
- Key Expiry: A Vending Key can be set with an expiry date
- Key Refresh: Keys must be refreshed every 30 to 365 days.
- Key Limits: Unit and Currency Limits

FILLING IN THE FORMS

Request for Vending Key Form

STS ASSOCIATION

Request to create a new Vending Key

Supply Group Code	123456	SGC that the vending key applies to
Supply Group Code Name	STS TEST SGC	
Key Type	2 - DUTK (Unique Key)	Select the key-type required
DKGA	DKGA = 04 (HMAC STS6 onl	For base date > 1993, use DKGA=04
Base Date	2014	
Activation Date	15/03/2019	When does the vending key become active
Credit Vending Expiry (KEN)	255	Leave as 255 if unsure
Expiry Date	01/01/2044 00:00	When does the key become inactive

Signed: Name: Date:

Simple ▸ Trusted ▸ Secure

STS ASSOCIATION

Key Use Authorisation Form

To be completed by the Supply Group Owner

SGC Owner Name:	STS Association	SM Purpose	Vending	◉	select applicable
Please allow the secure module with the SM ID below:			Manufacturing	○	
SM ID	94xxxxxx				
To use the vending keys of:		Module Type	Legacy	☐	select applicable
SGC Number	123456		STS6	✓	
SGC Name	STS TEST SGC				

From now until the key expiry date below: (leave blank if not an STS6 module)

Key Expiry Date	01/01/2044

After which date the KMS shall not permit the keys to be refreshed - the keys shall be excluded from the key use files issued to the Security Module after the above Key Expiry Date.

Note that the key expiry, refresh period, and vending limits ares only applicable to STS6 modules.

Refresh Period	60	Days until next key refresh
Unit limit per Key Revision	1000000	Max cumulative no of Units allowed to vend
Currency Limit per Key Revision	1000000	Max cumulative Currency amount allowed to vend

Signed:	Name:	Date:
SGC owner signature	SGC Owner name	15/03/2019

WHAT IS THE KMC PUBLIC KEY?

- For security purposes, your Vending System and the KMC need to trust each other. This is done by means of key sharing between the KMC and your security module.
- When you send the Key Authorisation form to KMC, you also need to send them a VkLoad request file. This needs to be generated by your updated Vending System.
- You will receive a VKLoad Response (similar to the old keyfile) which contains all the valid keys and versions thereof for your security module.

METER CERTIFICATION PRIOR 2012

- The TID rollover functionality could not be tested prior to 2014, due to a lack of appropriate testing infrastructure
- The TID rollover functionality has been a requirement since 1993, so all meters should comply
- There is a small risk that some of these meters might not behave correctly when a TID rollover key change is performed
- The STS Association will assist with identifying these meters and provide free of charge services to re-test samples of these meters

ACTION TO TAKE

- Upgrade the vending system and secure module to STS600-4-2 compliance
- Instruct meter vendors to supply any new meters on base date 2014
- Validate meters that were certified prior 2014
  - Replace non-compliant meters (list available from STSA)
- Do a key change on every meter
  - extend their life to 2045
- **STS METERS DO NOT NEED TO BE REPLACED**

KEY CHANGE OPERATION

- Demarcate meters into smaller groups
- Do a key change on one group at a time
- Set up a help-line front desk to deal with exceptions
- <u>OPTION 1</u>
  - Issue key change tokens to consumers when they purchase credit
  - Consumer enters the key change tokens before entering the credit
- <u>OPTION 2</u>
  - Issue key change tokens to trained technical team
  - Technical team visits each meter and enters the key change tokens
- **Start as soon as possible and spread the operation over a manageable period of time**

TID CONSERVATION

- Any technical solution that extends the life of the TID beyond 2024 (*Change the TID increment from 1 minute to 10 minutes), is* **NOT endorsed by the STS Association**
- Such a solution will render the vending system non-compliant to the STS specifications
- Serious security risk to propagate weakening vending keys beyond 2024
- Key management services and hardware secure module support for legacy STS will cease in 2024

ASSISTANCE FROM STSA

- A task team has been established to manage and advise on the TID rollover process
- Setting up a user discussion forum on the internet
- Communication with all STS users
- Providing guidelines to all STS users
- Assisting with meter certification (prior 2014)
- Visit http://www.sts.org.za
  - Email: Shawn O'Neill shawno@net1.com or
  - Dave Tarr Dave.Tarr@landisgyr.com

TID ROLLOVER

THE TIME IS NOW!

STS would like to remind all utilities, meter and vending systems manufacturers of the TID Rollover Timelines.

THE ROLLOVER PROJECTS MUST BE COMPLETED BY THE END OF 2023

STS ASSOCIATION

Standard Transfer Specification

Simple ▸ Trusted ▸ Secure

4 Karen Street, Bryanston West, Jhb, Gauteng, South Africa

+27 11 061 5000 | info @sts.org.za | www.sts.org.za

Simple ▸ Trusted ▸ Secure

STS ASSOCIATION

STS ASSOCIATION

STANDARD TRANSFER SPECIFICATION

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, c/o Van der Walt & Co.

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

Simple ▸ Trusted ▸ Secure

STS ASSOCIATION