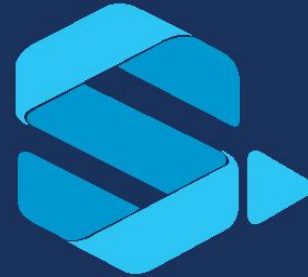


The 2019 General Meeting and PIESA- IERE South Africa Forum

Electricity & the 4th Industrial Revolution
– an Africa perspective



October 28 - 31, 2019



STS ASSOCIATION

Simple ▶ Trusted ▶ Secure

CRITICAL NOTICE AFFECTING ALL STS METERS
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

Simple ▶ Trusted ▶ Secure

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

Simple ▶ Trusted ▶ Secure



The TID and the meter

TID Count	Meter sees	When	mitigation
0	0	01/01/1993	n/a
1	1		n/a
....		n/a
99999	99999	24 Nov 2024	n/a
100000	0	Token replay when stack reset	Change key

TID Stack in the meter – last 50 tokens used

0 – most recent token

1 – second most recent token

..

..

..

49 - Second oldest token

50 – any token older than this is rejected

If you just cleared the TID stack without changing the meter key? If you do not clear the TID stack?

Simple ▶ Trusted ▶ Secure

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

Simple ▶ Trusted ▶ Secure



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**

Simple ▶ Trusted ▶ Secure



STS SECURITY LEVEL

- The National Institute of Standards and Technology (NIST) is the global reference for cyber security
- In 2005 NIST deprecated 56-bit cryptographic keys due to the risk of compromise by brute force attack
- STSA upgraded the STS security levels to 160-bit vending keys (published as STS600-4-2), which is approved by NIST for use up to 2045 (10^{32} times stronger)
- It is essential that current prepayment systems upgrade to the new security level as soon as possible

Simple ▶ Trusted ▶ Secure



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 TSM500 and TSM250 secure modules can be firmware upgraded to STS600-4-2 level
- 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

Simple ▶ Trusted ▶ Secure



METER CERTIFICATION PRIOR 2014

- 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 is assisting with identifying these meters and provides free of charge services to re-test samples of these meters

Simple ▶ Trusted ▶ Secure



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**

Simple ▶ Trusted ▶ Secure



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
- OPTION 1
 - Issue key change tokens to consumers when they purchase credit
 - Consumer enters the key change tokens before entering the credit
- OPTION 2
 - 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**

Simple ▶ Trusted ▶ Secure

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

Simple ▶ Trusted ▶ Secure



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.tidrollover.com>
 - Help line: tid@sts.org.za
 - [Scary](#).....

Simple ▶ Trusted ▶ Secure

There will now be a short presentation of some case studies on the TID rollover project and for that I would like to introduce Keseree Rajoo from Utilities World.

Thank you



Simple ▶ Trusted ▶ Secure





UTILITIES WORLD

SMART REVENUE MANAGEMENT SOLUTIONS

Presenter: **Keseree Rajoo**

Business Development Manager

29 October 2019

CASE STUDIES – TID PROJECT

Simple ▶ Trusted ▶ Secure



STS ASSOCIATION

ACTIVE SITES

Total of 9 sites that are currently active with their TID Projects

Emalahleni Local Municipality
Rand West City Local Munic Elec
JB Marks Local Municipality
Dr Beyers Naude LM
Greater Letaba Municipality
Ngwathe Local Municipality
Lekwa-Teemane Local Municipality
Richtersveld Local Municipality
BCM



Lekwa-Teemane
Local Municipality



GREATER LETABA
MUNICIPALITY



Expansion on two different approaches
by Municipalities shown next.



UTILITIES WORLD
SMART REVENUE MANAGEMENT SOLUTIONS

Simple ▶ Trusted ▶ Secure



STS ASSOCIATION

ACTIVE SITES

BCMM 5% COMPLETION



Installed Meters	Meters On KRN1	Meters On KRN2
130 073	123 076	7320

- Started 1 April 2019
- Currently working through a passive update
- Plan for active updates to start January 2020
 - through the municipal cashiers and various self-service options for the tech savvy customers,
- Project completion end 2020



Simple ▶ Trusted ▶ Secure



ACTIVE SITES

Beyers 55% COMPLETION

Installed Meters	Meters On KRN1	Meters On KRN2
11 604	5424	6 180

- Started 1 July 2019
- UW Project team on the ground actively updating via the audit app
 - House to house sweep audits and updates
- Projected completion date - end 2020
- Municipality wants increased revenue and thus took on the active update approach.



Simple ▶ Trusted ▶ Secure



TID Checklist

- ✓ Vending system provider STS 6 compliant / certified
 - ✓ System updated and new key (KRN 2) applied for
- ✓ Meter suppliers STS 6 compliant
 - ✓ Inform that all new meters must be on KRN 2
- ✓ All meters in stores and with contractors key changed
 - ✓ Or key change on installation
- ✓ Develop an active update strategy with vending provider
 - ✓ Advertising to the public is key – they MUST use all their old tokens
- ✓ Deploy the strategy
 - ✓ Measure, monitor – this should be a KPI for the next four years



UTILITIES WORLD
SMART REVENUE MANAGEMENT SOLUTIONS

Simple ▶ Trusted ▶ Secure



STS ASSOCIATION

PREFERRED APPROACH

- Municipal Cashier Terminals – ring-fenced, controlled environment, makes for easier control and distribution of Key Change Tokens to customers
- Cashier & Customer education can be better managed
- Building awareness through marketing and advertising in and around the municipal cashier terminals can be better facilitated.
- TID appointed ambassadors can be positioned strategically to assist customers before they receive their tokens.
- Support is also better managed as the areas are predetermined and thus everyone's efforts are targeted to specific areas at any given time.



UTILITIES WORLD
SMART REVENUE MANAGEMENT SOLUTIONS

Simple ▶ Trusted ▶ Secure



STS ASSOCIATION

THANK YOU!

UTILITIES WORLD

SMART REVENUE MANAGEMENT SOLUTIONS



Keseree Rajoo

Business Development Manager - Intl

701 Strauss Daly, 41 Richefond Circle, Ridgeside,
Umhlanga, 4319

Tel: +27 31 833 0100 **Cell:** +27 71 064 5577

Email: keseree@utilitiesworld.co.za

www.utilitiesworld.co.za

Simple ▶ Trusted ▶ Secure



STS ASSOCIATION