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

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

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

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

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

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

- Established a task team to manage and advise on the TID rollover process
- Launched a dedicated microsite
- With discussion forum & Chatbot for Communication with all STS users
- Providing TID Rollover guidelines to all STS users
- Assisting with meter certification (prior 2014)
- Visit http://www.tidrollover.com

HELP LINE: TID@STS.ORG.ZA

Simple ▸ Trusted ▸ Secure

STS ASSOCIATION

STS ASSOCIATION
Standard Transfer Specification

INTRODUCING
TID ROLLOVER WEBSITE

www.tidrollover.com

The STS Association has developed a new centralised website for all TID Rollover communication. The website will highlight TID Rollover specific campaign updates, training and workshop invitations, TID guideline videos, inspire urgent and critical call-to-action, offering an instant chat box and will also house a forum for all queries and frequently asked questions.

Simple ▸ Trusted ▸ Secure

www.sts.org.za | www.tidrollover.com

STS ASSOCIATION

STS ASSOCIATION
Standard Transfer Specification

INTRODUCING
STS YOUTUBE CHANNEL

@ sts_association

The STS Association has developed a new centralised website for all TID Rollover communication. The website will highlight TID Rollover specific campaign updates, training and workshop invitations, TID guideline videos, inspire urgent and critical call-to-action, offering an instant chat box and will also house a forum for all queries and frequently asked questions.

Simple ▸ Trusted ▸ Secure

www.sts.org.za | www.tidrollover.com

STS ASSOCIATION

THANK YOU

Simple ▸ Trusted ▸ Secure

STS ASSOCIATION