Critical notice affecting all STS meters

Token ID rollover event in 2024

Don Taylor **Chair - STS Association**

19 July 2018

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 calculated as the number of minutes that have elapsed since a base date of 1993
- The meter records the TID when it is entered into the meter to prevent token replay

STS ASSOCIATION

Limitations of the TID

- The TID is encoded into the token as a 24-bit binary number
- It 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

STS ASSOCIATION

TID size trade-off

- Why was the TID not designed to last longer than 31.9 years?
- A larger TID would mean a smaller field for Transfer Amount and reduced resolution
- It is normal practice to upgrade the cryptographic strength at least every 30 years
- This means that the meter cryptographic key would need to be changed within this period in any event
- 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 ASSOCIATION

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
- 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 has been a requirement since 1993, so all meters should comply
- The TID rollover functionality could not be tested prior to 2014, due to a lack of appropriate testing infrastructure
- 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

- **METERS DO NOT NEED TO BE REPLACED**

STS ASSOCIATION

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

STS ASSOCIATION

TID conservation – a serious issue

- A certain company is promoting a technical solution that extends the life of the TID beyond 2024
  - Change the TID increment from 1 minute to 10 minutes
- STS Association does NOT endorse this method
- Renders the STS vending system non-compliant
- Serious security threat to propagate weakening vending keys beyond 2024
- Key management services and hardware secure module support for legacy STS will cease in 2024

Supply of secure modules

- Single supplier currently
  - One more this year + one potential next year
- STSA cannot discuss pricing - Competition Act contravention – advice from legal counsel
- Has to be negotiated with suppliers
- AMEU could discuss a workable model with Prism on behalf of its members
  - Contact: Shawn O'Neill 083 262 8802 <shawno@zazooltd.com>

Pricing of secure modules

- STSA did a survey of SM suppliers internationally
  - They all use pricing model of an annual license fee
  - Prices are in line with what Prism is offering
- STSA negotiated the model with Prism last year
  - Low volume use: per transaction fee
  - High volume use: annual license fee (includes maintenance)

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: Don Taylor <dt@almegatec.co.za>

STS ASSOCIATION

THANK YOU FOR YOUR ATTENTION