Securing your Prepayment Solution from the Potential Threat of Ghost Vending

1. Introduction

Nearly twenty years after its inception in 1993, the Standard Transfer Specification (STS) protocol has grown to its current status as the de facto solution for one-way pre-payment. To date more that 400 utilities in 30 countries are utilizing this system to provide a vending channel for over 10 million meters. The protocol has been stable for more than 15 years and is has become recognised as the only globally accepted standard for pre-payment, ensuring inter-operability between components from different manufacturers of pre-payment systems and meters. Originally developed for the South African environment to provide an effective means of dispensing electricity to medium & lower income households, it is now rapidly growing in the international market as well.

New developments has seen the technology adapted for gas as well as water meters and updates to the protocol will soon cater for two-way prepayment & complex tariffs.

Despite the undeniable success of the STS system, a phenomenon known as “ghost vending” has unfortunately been confirmed as a potential revenue protection threat. This paper will analyse the security inherent to STS, explain the methods used by criminals to enable ghost vending and then give clear guidelines on how to identify risks & prevent this threat from impacting your business.

This paper will underpin the reality that taking pro-active measures by investing in the correct solutions and best practices, the future success of your pre-payment infrastructure can be guaranteed.

2. The STS Components & Functions

Most people are familiar with a pre-paid meter, the vending point and the STS token, but what is not always as clear is how all these elements tie together. A better understanding of these relationships and the security of the system is the first step towards combating potential threads.

The STS system transfers credit from a vending point to the meter by a special secure encryption of the information. The output is a 20 digit code that is entered into the meter. The meter is able to decrypt the token and then update the credit register ONLY if all parameters contained in the token are successfully validated. The meter manages this with a special *Meter Key,* which it shares with the security module of the vending system. The meter key is built into the meter during the manufacturing process and is programmed with the following important parameters:

- *Meter Serial Number* – The value is inherent to the meter and can only be changed with a firmware upgrade. The meters will only accept a token from a vending point with the correct meter serial number.
- *Supply Group Code (SGC)* – This is a unique number that is allocated to a utility by the STS association and is shared by a group of meters. (Some utilities may have several meter groups based on geographical area or commercial profile.) The meters will only accept a token from a vending point with the same registered supply group. The supply group can be updated on the meter by entering a special key change token. The only way to change to a new supply group is by requesting a new Vending Key from the Key Management Centre. (see later)
- *Key Revision Number (KRN)* – A number that is associated with the particular revision of the Vending Key (in the security module) and the Meter Key in the meter. This number is also managed by the Key Management Centre and can only be updated by requesting a special file from the centre.
- *Tariff Index (TI)* – The tariff number is allocated to a particular consumer group(s) and it is managed by the vending system. It is not under the control of the STS association and tariff tables can be defined by the utility. The meters will only accept a token from a vending point with the correct tariff index.

- *Token Identifier (TID)* – This number is a time stamp that logs the number of minutes that have elapsed since 1st January 1993. It is coded onto the token by the security module when the vending transaction is processed. The meter will check this number to ensure it is impossible to re-use a token.

(Note that the token encrypts additional parameters including the manufacturer code, ISO BIN etc, but this detail is not important to the rest of the discussion)

When a client goes to a vending station to buy a token the details are relayed to the back end vending system. The vending system will retrieve the relevant data (MSNO, Tariff Index) from the database and send this information along with the specified credit value to the security module. The security module will now generate the TID and encrypt all the information into the token using the Vending Key and Meter Key. It is important to note that the *Supply Group Code* as well as the *Key Revision Number* is not visible to the vending system. These values are secured inside the Vending Key of the security module. Neither the utility, nor the vending supplier can change the values without a special request for an encrypted file issued from the Key Management Centre.

The 20 digit token is issued and either printed on a customer receipt or loaded on a magnetic card for transport to the meter. When the meter decrypts the token, it will validate each of the parameters listed in the previous section. If any of the parameters retrieved from the token do not agree with the values programmed on the meter key, the token will be rejected. The meter will also compare the TID to the last 50 values stored in memory to ensure the token has not previously been used. Only after all validations have been passed, will the meter update the register with the credit value received from the token.

The security module is therefore the most important piece of hardware in the vending cycle. This unit is a small device manufactured by Prism for the Key Management Centre (KMC). The device is physically secure and stores one or more Vending Keys as well as the Key Exchange Key. These keys are used to manage all the encryption and decryption functions. The vending key(s) can be updated through a special file that the Key Management Centre issues to registered service providers on special request, but the Key Exchange Key can only be loaded onto the security module inside the premises of the Key Management Centre. Neither the vending supplier nor the utility have any control over this process. The security and related keys for every STS module in the entire world is managed solely by the Key Management Centre located at ESKOM headquarters in Megawatt Park, South Africa.

Even this simplified high level overview of the STS process should clearly convince the reader of the comprehensive controls that are in place to prevent fraud. How then did ghost vending get a foothold?

3. What is Ghost Vending?

Ghost vending is the illegal practice of selling credit tokens to pre-paid clients from rogue vending stations not affiliated or linked to with the supply utility and then pocketing the money. From the previous discussion its clear that the meter will only accept a token if all the key parameters are validated. The only way to ensure this ability is by being in possession of a registered security module set up with the keys and codes that are shared by the meters in the field.

The origin of ghost vending can be traced to the earlier vending solutions that allowed for off-line vending stations. The vending points could generate tokens even if it was not linked to the back-end system, because a physical security module was installed inside the computer at the premises of the vending station. If the vending machine and security module fell into the hands of criminal elements it was possible for them to issue tokens without connecting to the central system. Most of the vending software addressed this risk by introducing a credit limit. The vendor bought bulk credit upfront from the vending supplier. This credit was loaded on the vending machine and it would now be possible to issue tokens until the credit was depleted. The software will then prevent the issuing of additional credit tokens. The vendor first had to reconcile the money received before he was again allocated credit to load onto the vending terminal. This system gave reasonable security but in practice the following risks existed:

- Not all implemented vending software solutions had this credit limit functionality.
- The loading and consolidation of credit was an involved process that had to be carefully managed. There were instances where the feature was disabled.
- The credit limit was managed by the software, not by the security module. A technical specialist with intimate knowledge of the vending software could circumvent this feature.

Criminal syndicates targeted vulnerable vending stations to get hold of the security modules. Instances of physical break-ins at shops or even government offices that sold electricity were reported. There were also reports of old vending machines stolen from storage. Even with the vending machine and security module, the user still needs a good understanding of the processes, software and data systems to generate these tokens. Good suspicion therefore exist that the syndicates are either run, or alternatively employ the services of former inside operators.

If a syndicate had an offline vending machine with a security module in its possession, along with the technical expertise to operate the system, it now had the means of generating illegal tokens.

The practise would be to offer the client a credit token at a large discount. The user would be able to enter the token on his meter without compensating the utility for the electricity consumed. The money offered for the "cheap" token would go directly to the pockets of the criminal syndicate.

The true extend of the problem is not entirely clear, but the total fraud may be estimated at millions of rands. Two men were sentenced in 2011 for masterminding a syndicate that sold up to R10 million worth of electricity tokens to ESKOM clients. They were handed jail terms of 18 & 15 years respectively. The group was in possession of four vending machines.

To put this in perspective, ESKOM has reported that up to 58 vending machines may have been stolen, of which only 18 have been recovered. That means 40 vending machines may potentially be in the possession of criminal elements.

This practise is not limited to South Africa. A revenue protection investigation in a ring fenced area in an African utility confirmed that up to 10% of the meters out of sample of 1000 meters were getting credit from ghost vending points. This could be established by credit changes on the meter without any transactions registered on the vending system.

4. Ensuring Your System is Secure

The most important safeguard against ghost vending is the protection of the security modules. With the modern vending solutions provided by the leading suppliers there is no reason that a security module needs to be in the field where it is vulnerable to theft. Where the old offline systems required a large number of in field security modules, many installed at remote satellite vending stations, the current solutions are able to offer the same service with only 2 centralised security modules that serve the vending requirements of a typical medium sized utility.

The modules are hosted in a very secure environment that is only accessible to few authorised individuals. The leading suppliers now offer multiple vending channels including cellular networks, ATM machines and the cash points at major retailers. These pay-points request the encrypted token via online communication networks from the central system, so there is no outside access to the secure keys. This makes it impossible to generate a fraudulent token.

The second important fact to note is that a security module is paired only with meters that are programmed with the same Supply Group Code and Key Revision Key as is embedded in the vending key of the module. That means an old stolen security module from another utility will not work on your meter population.

The vending key can only be updated through a special file that is supplied by the Key Management Centre. The leading vending suppliers understand the importance of managing these keys and modules. Any utility expanding its prepaid footprint or even embarking on a new pre-paid venture needs to ensure that the chosen supplier of the vending solution has the experience, best practices and technology to provide this security.

Taking the basic lessons learned from the past and implementing the correct solutions & preventive measures, will ensure that ghost vending is not a threat to your prepaid solution.

5. Recognising & Combating Ghost Vending

So how should a utility coming from a legacy vending solution check for potential ghost vending activity; and if confirmed what would be the course of action to eliminate.

A properly constructed Revenue Protection program that utilizes business intelligence tools will be able to pinpoint ghost vending. The first step will be to always capture the remaining credit displayed on the pre-paid meter as one of the data fields retrieved from any field inspection. These readings should be compared in the back office against a dataset of the historic vending transactions. The first "flags" will be raised by meters with remaining credit, but without any recent vending activity, or only relatively small and infrequent vending transactions that do not correspond to the credit values on the meter and the expected consumption of the end consumer. Software that automatically performs these statistical comparisons on the data downloaded from field inspections will quickly be able to highlight a list of high risk meters. This is also why it's recommended that field inspections are processed on an electronic hand held unit. Paper forms could potentially contain errors (transposition or otherwise) and make it slow and tedious to analyse findings.

The list of high risk meters should then be used to perform a targeted follow up inspections a few weeks later. With the base line reading from the first inspection recorded, any positive change on the credit reading of the meter that do not tie up with the total value of vending transactions will confirm suspicion. Ghost vending can now be proven by analysing the TID stack recorded in the meter.

The STS pre-paid meter records the last 50 Token Identifiers (TID's) in its memory. As previously discussed, this unique number is generated through the security module when the vending transaction is processed. The vending system database also keeps a record of the TID numbers for all tokens issued. The suspicious meter may be removed and the data can be downloaded from a test bench. If any TID record(s) found on the memory of the meter, do not match the TID records on the vending database, it is positive proof of ghost vending.

When a utility knows that ghost vending is happening in an area, there are practically two ways of stopping this activity. The first option is to find the ghost vending station, or more importantly the stolen security module. As was explained earlier, a valid token can only be generated by a security module with the specific vending keys linked to those meters programmed with the matching supply group code and key revision number. Removing the security module takes away the possibility of creating tokens. The revenue protection officer has positive proof which clients purchased a token from an illegal station, so with investigation work it may be possible to trace the station. This may unfortunately not be that easy. The syndicates typically move around frequently, to avoid detection. Furthermore the threat can only be totally eliminated if ALL security modules are accounted for. If the utility does not have complete records and can account for every security module since the vending program was initiated, it may be difficult to have complete security.

The second option is to re-program all the infield meters so that they are no longer compatible with the original supply group (or key revision number). In this process the first step will be to invest in a trusted vending supplier with multiple vending channels, without the need for any offline vending points. The upgraded security modules must be hosted in a secure facility with excellent access control for select individuals. A program may now be launched to systematically update the keys programmed in the meters.

The vending supplier will request a new supply group (or key revision number) from the Key Management Centre. This new code is known only by the vending supplier and the Key Management Centre with the details of encryption never leaving the Key Management Centre. The new vending key with the updated supply group is supplied to the vendor after the necessary application procedures and security checks. The new vending key is locked in an encrypted Key Load file. The vending supplier uses this file to add the updated key to their security module(s).

The modern security module may have multiple vending keys. So it’s now possible to migrate the meters systematically from the old supply group to the new group. The security module can issue a key change token. (It can only issue this key change token for the new group with the new loaded key). The field operator enters this special key into the meter to change the supply group. From that moment forward the meter will not accept any credit tokens based on the previous supply group. Any token issued from the ghost vending station will be rejected by the meter. This is obviously a tedious process as each meter needs to be visited and may require substantial field work depending on the meter base size.

It is recommended that the issuing of the key change tokens and the field process of entering these values into the meters are coordinated by a proven works management system. The utility must keep careful track of the end-to-end operations and confirm when a meter was updated. Leaving this process to an end user client prevents any traceability or feedback conformation. If the end user neglects to enter the new key, or enters the key incorrectly, the meter can still accept the ghost vending credit tokens. Even worse, if the utility moves the meter record now to the new key on the vending system, the client can't receive a token from the approved vending points and will depend solely on the ghost vendor.

A works management system integrated to the vending system database will be able to close the loop and ensure all meters are updated over a period of time.

6. Conclusion

The threat of ghost vending is real and large amounts of money have been lost due to this practise. The problem is the product of highly organized syndicates exploiting past mistakes and shortcuts taken in the vending security chain. The well managed STS vending solution is extremely secure and it has proven to be the preferred technology worldwide. The utility can guarantee the ongoing benefits offered by pre-payment by adhering to the following principals:

- Invest in a proven vending system with all the required security features.
- When partnering with a vending supplier, ensure that they have securely managed processes and the capability of providing the highest possible security around the security modules.
- Move away from any offline vending stations to fully online solutions that utilise security modules in a central secure site. Advances in modern technology and communication infrastructure have rendered offline stations obsolete in just about all circumstances.
- Make sure that all security modules are accounted for through their entire lifecycle. Even older modules no longer in use may be a risk. Vending stations & security modules lying somewhere in a storeroom may be a temptation for the criminals
- Ensure that your revenue protection program has the right proven business intelligence and analytical tools to quickly highlight potential problems through electronic data analysis.