STS6 Vending TSM500i NSS User Guide

August 2023

Document number:	PR-D2-1126 Rev 1.1
Release date:	August 2023
Copyright:	© 2023 Prism Payment Technologies (Pty) Ltd
Synopsis:	This document describes the PCI HSM v3.0 STS6 Vending TSM500i-NSS Hardware Security Module (HSM), and the TsmWeb and PrismToken interfaces used to manage this HSM.

Important Notes

⚠️ **This document only applies to a STS6 Vending TSM500i that has Boot Loader v1.5.0.0 or later. Earlier versions of the boot loader do not have the same dual control requirements as mandated by PCI HSM v3.0. Refer to document no. PR-D2-0854 "TSM500i and TsmWeb User Guide" for an HSM with BL v1.2.x.x or BL v1.4.x.x.**

⚠️ **The TSM500i should always be transported in its original packaging (in an anti-static bag in foam padded box). <u>Failure to do so could result in damage to the HSM</u>. The original packaging should be kept in a safe place in case it becomes necessary to transport the HSM to a different location.**

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

Contents

1 Overview

The STS6 Vending TSM500i-NSS is a Hardware Security Module (HSM) and is also referred to as the TSM or HSM in this document. These terms are used interchangeably in the remainder of this document. **This document only applies to the STS6 Vending TSM500i-NSS that has Boot Loader v1.5.0.0 or later.** The STS6 Vending TSM500i-NSS supports full STS6 functionality that includes: -

- Key management functions (i.e. generate VKLOADREQ, upload key load file, delete vending keys etc)
- Vend STS Management Tokens
- Vend STS Key Change Tokens
- Vend Credit Tokens

1.1   TSM500i-NSS Description

The TSM500i-NSS is a network appliance that includes a TSM500i HSM packaged together with an embedded computer system. This solution has an Ethernet interface and includes a serial interface for loading CSPs. An LCD display provides basic status information.

The embedded computer system in a TSM500i-NSS is pre-installed with the following: an interface service called **Conductor**, the **TsmWeb** application and supporting drivers. Below is a simplified view of what is inside the TSM500i-NSS and how it inter-connects.

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za
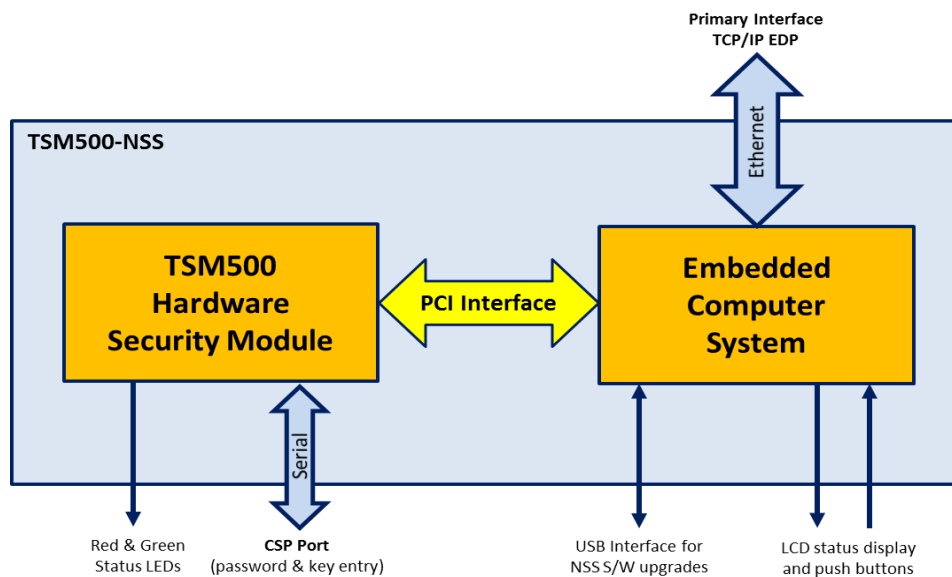
The TSM500i-NSS hardware version 5520-00130_v1.1_NSS looks like the picture below.

TSM500i LEDs   KCED PORT

Hardware version: 5520-00130_v1.1_NSS

The TSM500i-NSS hardware version 5520-00130_v1.2_NSS looks like the picture below.

TSM500i LEDs   USB PORT (NSS software updates)

Hardware version: 5520-00130_v1.2_NSS

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

2 Setup Quick Guide

(See 3.1)

Inspect and Install Hardware
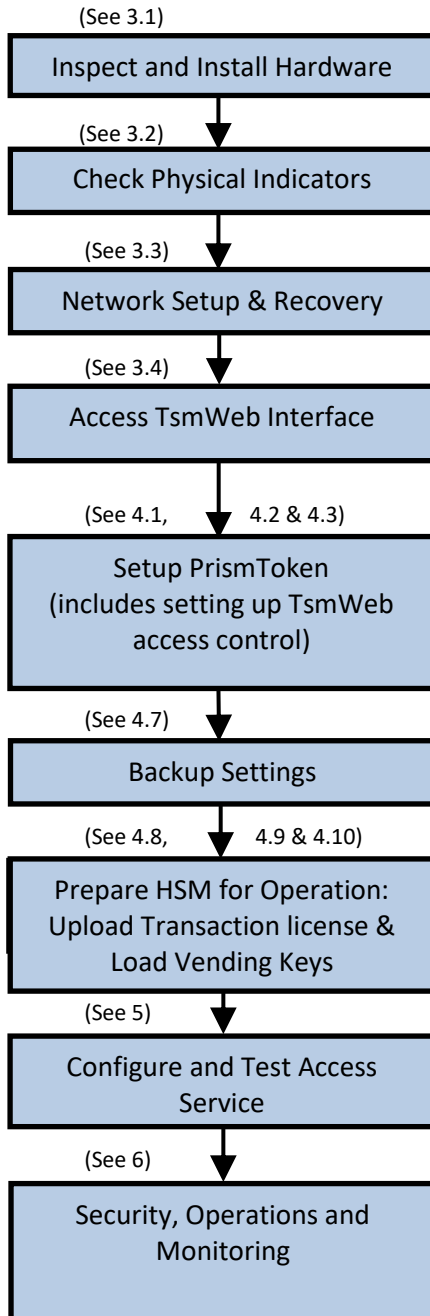
The TSM500i NSS hardware must be inspected and then installed in a secure environment.

(See 3.2)

Check Physical Indicators

Power on and check physical indicators (LEDs) to confirm that the hardware has been successfully installed.

(See 3.3)

Network Setup & Recovery

Set the IP address, network mask and default gateway using the LCD Menu which is accessed via the front panel.

(See 3.4)

Access TsmWeb Interface

Enter the IP address into a web browser on a PC that is connected to the same subnet to access TsmWeb. Set the TsmWeb admin user account password. Login to TsmWeb as admin and perform a basic functionality test.

(See 4.1, 4.2 & 4.3)

Setup PrismToken (includes setting up TsmWeb access control)

Upload the PrismToken License (emailed by Prism), setup TsmWeb access control by creating TsmWeb user accounts and set account expiry dates, setting the password policy and default auto-logoff times, and setup PrismToken Users. *If not using PrismToken , then communication with the HSM is via the conductor interface, see 4.5 for more detail.*

(See 4.7)

Backup Settings

Follow the backup procedure to backup TsmWeb settings.

(See 4.8, 4.9 & 4.10)

Prepare HSM for Operation: Upload Transaction license & Load Vending Keys

Access the PrismToken dashboard and navigate to the key management tab to upload the transaction license and KMC Public Key into the TSM500i HSM. The vendor will be required a completed KUA form (for each vending key required) and a VKLOADREQ to the live KMC. The KMC will respond with a keyload file (KLF) that contains live vending keys. The KLF can be uploaded into the HSM via the PrismToken key management tab.

(See 5)

Configure and Test Access Service

Client software must be configured to communicate with the Thrift API service or conductor service (if PrismToken not being used). Testing needs to be to ensure that transaction processing can proceed successfully. Third-party tools will be used during this step.

(See 6)

Security, Operations and Monitoring

Operate PrismToken securely by restricting access to those clients/networks that need it. Do not expose PrismToken/TsmWeb/NSS to the internet. Use strong passwords for all PrismToken/TsmWeb accounts. For reliable operations establish and perform the recommended regular monitoring checks, at least once a week. Establishing a Disaster Recovery (DR) plan with a standby PrismToken and Security Module is strongly recommended to ensure vending system availability.

This section defines the customer's responsibilities on receiving TSM500i HSMs to ensure that security is maintained during the delivery process.

3 NSS Initial Setup

3.1 Inspect and Install Hardware

3.1.1 Hardware Inspection

This section defines the customer's responsibilities on receiving TSM500i HSMs to ensure that security is maintained during the delivery process.

- Verify that the goods arrive via the same waybill number as per what was supplied in an email from Prism.

- Verify that the packaging and TSM500i-NSS HSM has not been tampered with in any way by confirming that tamper evident stickers on the packaging and hardware are intact. Also verify that is no sign of physical damage.

- Verify that the hardware has not tampered. Power on hardware and if red status LED is permanently ON then the hardware has tampered.

- Unpack and verify contents of the KCED packaging. Refer to *Key Component Entry Device (KCED) Installation & User Guide.pdf (0560-00157)* for more details.

Contact Prism immediately if the serial tamper evident stickers have been interfered with, or if the HSM is in the tampered state. An HSM that arrives in the tampered state cannot be authenticated and should be returned to the Manufacturer.

3.1.2 TSM500i-NSS Hardware Installation

- Connect an Ethernet patch cable (not supplied) from your network hub to the port labelled "ETHERNET" on the rear panel of the TSM500i-NSS.

- Connect the mains cable from your mains supply to the socket labelled "100−240 VAC".

3.2 Check Physical Indicators (LEDs)

After powering on the TSM500i-NSS check status LEDs that are located on the front panel.

⚠️ **The red and green status LEDs provide <u>very important</u> information about the current state of the TSM500i.**

The meaning of these LEDs **must be understood,** and the LEDs should be monitored when performing management functions on the TSM500i.

During **normal operation**, the **RED LED will be OFF,** and the **GREEN LED should be FLASHING** (either 1-flash if in *Loader* state or 2-flash if in the *Operational* state).

A detailed description of the LED states is given below:

RED	GREEN	Meaning
OFF	2-FLASH	**Application running**. This is a healthy operational state.
OFF	1-FLASH	**Loader state**. This is a healthy maintenance state. If the module is required to be in the operational state, it will need to be reset.
ON	1-FLASH	**Tampered state**. Remove and physically inspect the module (according to standard security procedures). Refer to the HSM's User Guide on how to clear the tamper condition.
OFF	ON	**Notice Me**. Typically this is a healthy operational state and indicates that the TSM500i is waiting for key/password entry (with a specified timeout period).
OFF *	ON	**Initialising and performing self-tests**. Occurs on power-up and reset. * Although the RED LED will remain off during initialisation / self-tests, it will flash once at the start of the initialisation sequence.
1-FLASH	1-FLASH	**Error state**. If resetting does not rectify the situation, contact Prism Support.
ON	OFF	**Corrupt state**. If resetting does not rectify the situation, contact Prism Support.
OFF	OFF	**Power is off or catastrophic hardware failure**.

Notes:

- Red ON or FLASH indicates that the HSM is unable to operate normally.
- Green FLASH indicates that the HSM is accepting commands.
- Green ON indicates that the HSM is busy.
- Both OFF indicates no power or a catastrophic failure.
- A 1-FLASH sequence follows the pattern 101010 (500ms per state)
- A 2-FLASH sequence follows the pattern 101000 (500ms per state)

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

3.3 Network Setup and Recovery

The IP address of the TSM500i-NSS will be displayed on the LCD on the front panel after powering up. The network setting factory defaults are:

IP address   192.168.0.201

Network mask   255.255.255.0

Default Gateway   "none"

If it is not possible to connect to the TSM500i-NSS over the local network, the IP address and network mask (netmask) can be changed via the front panel of the NSS using the *LCD MAIN MENU* (see section 3.3.1). The alternative is to access the NSS using the default address and change it later using the TsmWeb interface.

It is also possible to use the LCD Main Menu to reset the configuration to its defaults, reset the NSS to factory state and to reset the TsmWeb admin password.

3.3.1 Use the LCD MENU to set the IP address

To access the LCD MAIN MENU, power the TSM500i-NSS off. Power it on again and watch the LCD display. After about 30 seconds, the following prompt will be displayed briefly: "✓ + ✗ for menu…". Press and hold down the red ✗ button and green ✓ button on the front panel until a MAIN MENU appears on the LCD display.

Hint: You may hold the ✗ and ✓ buttons from before the prompt is displayed. However, you must keep the buttons depressed until the MAIN MENU appears.

The menu has the following layout, whereby the following menu options may be accessed by means of the up/down arrow keys:

MAIN MENU

1. Exit & Boot

2. TCP/IP   (includes IP address, netmask and default gateway setup)

3. TLS settings   (includes enable/disable and resetting of TLS key)

4. USB Backup   (includes options to backup and restore database)

5. Reset…   (includes options to reset Admin Password and config settings

To abort and proceed with the normal power-up sequence, select *Continue boot*.

Use the arrow keys and green accept key to select the **TCP/IP** option. This menu will allow the setting of the IP address, netmask and default gateway.

To change any address (IP address, netmask or default gateway), use the left and right arrow buttons on the front panel to move the cursor, until the cursor is under a digit to be changed. Use the up and down buttons to set the digit to the required value. Repeat the process for all digits in the address.
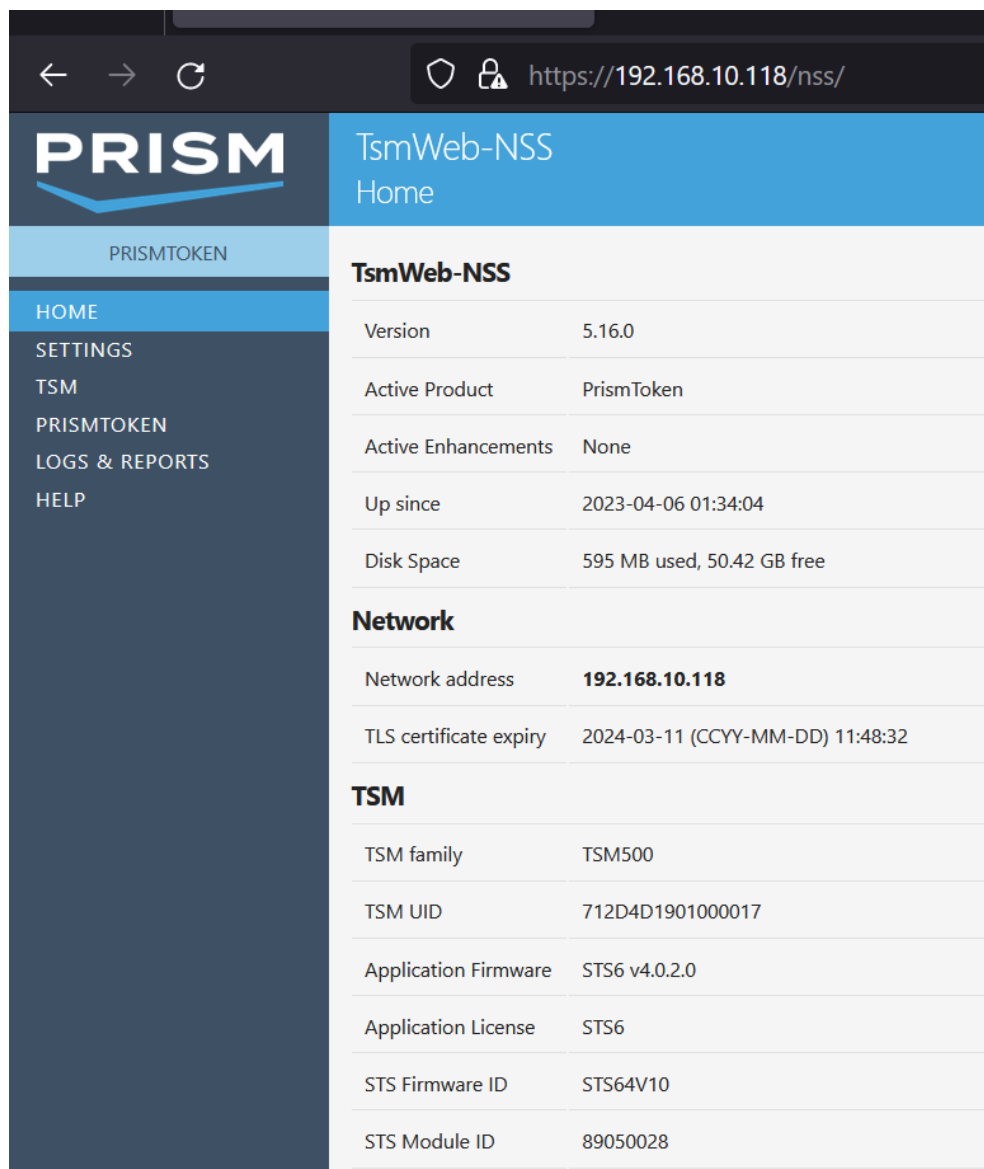
More details about the MAIN MENU can be found in section 9.1.

3.4 TsmWeb Interface

TsmWeb works best with Chrome and Mozilla Firefox web browsers. Internet Explorer is not officially supported.

3.4.1 Invoking TsmWeb for a TSM500i-NSS

When using a TSM500i-NSS, verify that the LCD on the TSM500i-NSS displays "TSM500-NSS READY" and that it also displays its IP address. Enter this IP address into a web browser, e.g. http://192.168.0.201/ on a PC that is connected to the same subnet to access TsmWeb. The home page similar to the one shown below should load. (The IP address entered must match the IP address shown on the TSM500i-NSS LCD).

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

3.4.2   Setting the TsmWeb admin password

Please note that TsmWeb is not supplied with default passwords, and it is necessary to <u>set a password</u> for the pre-defined *admin* username before using TsmWeb.

⚠️ The TsmWeb user account passwords must not be confused with, and are not related to, the Cryptographic Officer passwords that reside in the TSM500i HSM.

When using TsmWeb with a TSM500i-NSS, it is necessary to Login to TsmWeb in order to access any of the menus other than the *Home* page. The web browser will be re-directed to the TLS-secured log-in page. A warning will first be displayed due to what is believed to be an untrusted connection. The reason for this is that the certificate is self-signed so this warning can be ignored. In Chrome simply click "Proceed anyway". In Mozilla Firefox an exception will need to be added after clicking "I understand the risks".

ⓘ   All pages other than the home page are TLS-secured.

3.4.2.1   Setting Admin Password for the first time

If no admin user password has been set, the user will be presented with a screen titled **TsmWeb Set Admin Password** and with the following message in red text:

  "No password has been set for account 'admin'. Please set one now."

The username for this account is **admin** (case sensitive) and the user must enter a password for **admin**. The password must be entered into BOTH boxes provided in order to confirm the new password. Then click **Set Admin Password** to set the **admin** password.

Once a password has been set for the **admin** user, the **TsmWeb Log In** screen will be displayed. You may then login using username **admin** and your chosen password.

By default, the password must contain at least 7 characters and must include at least one of each of the following:

- Upper case character
- Lower case character
- Digit

⚠️ The default admin account will be set by default to expire 1 year from the date when the password is set for the first time.

3.4.3   Using TsmWeb for the first time

Enter the username (admin) and your newly assigned password and click Login .

Click **TSM** from the left side menu, wait for the *TSM Management* page to load.

If the Access control mode is **BL:TAMPERED_ROLE_NONE** then it means that the TSM500i is in the tampered state. If the HSM is tampered on arrival at the point of first deployment, it should be returned to the Manufacturer.

If the Access control mode is **BL:ERROR** then it indicates that the TSM500i has detected a hardware fault. If the problem is persistent after power-cycling, the unit must be returned to the Manufacturer.

> ⚠ **TsmWeb will automatically log the user off after a default of 10 minutes of inactivity.**
> **This timeout period can be configured via** *Settings > Preference Manager* **page on TsmWeb.**

> ⓘ When using TsmWeb on a TSM500i-NSS, you will always be required to enter a password.
>
> Refer to sections 3.4.2 and 4.2 for details on how to setup a TsmWeb admin password and further user passwords.

3.4.4   Accessing TsmWeb through a different subnet

In some instances, it may be necessary to access TsmWeb interface through a firewall or from a different subnet. Ports 80 and 443 will have to be enabled for incoming connections on the firewall if you need to access TsmWeb through the firewall.

When your client computer is on a different subnet, the TSM500i-NSS will need to have a default gateway specified. The default gateway needs a route entry that will correctly direct return network traffic from TSM500i-NSS to the remote computer you are using.

Select **Settings > Network** from the side menu, wait for the *Network* page to load.
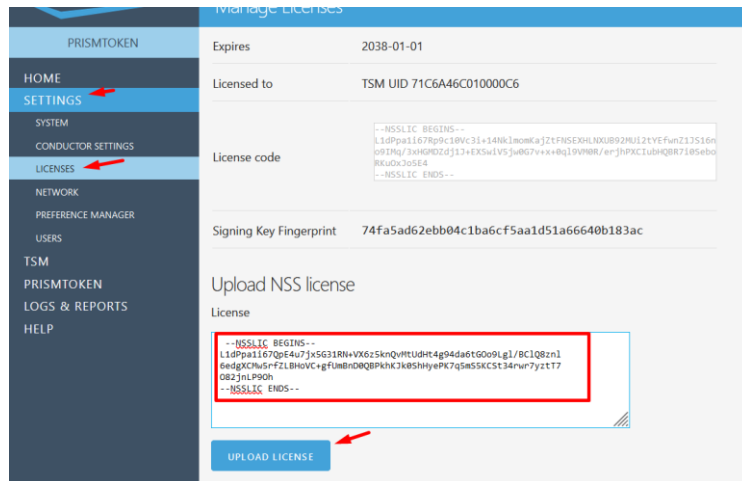
Click on the ≡ TASKS button on the "NSS Network Properties" pane and select Change Network Settings. Change the default gateway to the IP address of the default gateway, where your TSM500i-NSS is installed, and click Change .

4 TsmWeb Initial Setup

4.1 Upload PrismToken License Certificate

Log into TsmWeb as a user with the 'admin' role (for example, the 'admin' user)

Navigate to the **Settings > Licenses** page.

Copy the PrismToken license certificate (supplied via email by Prism) and paste it into the "License" field above the "UPLOAD LICENSE" button. Include the BEGIN/END lines.

Navigate to the **Settings > System** page. Click on "REBOOT NSS" for the license to take effect. Click on "YES, REBOOT NOW"

After the reboot, log into TsmWeb as a user with the 'admin' role and confirm that **PrismToken** is visible on the navigation bar on the left.

> ⚠️ **Once the PrismToken license is active, all communication to the HSM is done via the thrift API over a secure TLS connection on port 9443.**

4.2 Setup TsmWeb Users

4.2.1 Create users

Each TsmWeb user account should uniquely identify one user. No account should be usable by more than one individual.

To create a new user account, go to the **Settings > Users** page and click on the New User link. Enter all the new user's details. The user should then enter their password in the "New password" and "Confirm new password" fields.

> ⚠️ **Warning Note if the Account expires field is left blank then the default expiry is 1 year from the day the account is created**. The format for this field is YYYY-MM-DD.
>
> Once the user account expires the user will no longer be able to login to TsmWeb.

Set the account expiry to a suitable future value greater than 1 year from the account creation date

4.2.2   Configuring Account and Password Policy

TsmWeb account and password policy is configured in the *Preference Manager* which is accessed by navigating to the **Settings > Preference Manager** page. This will load a page listing the preferences that can be managed by a user with an **admin** role. The preferences are listed in alphabetical order. To find out more about a particular preference move the mouse cursor over the preference name and additional information will be displayed.

Review the values of all preferences starting with "account." and those starting with "password." to ensure they meet your requirements for your organisation and/or PCI-DSS compliance (if applicable).

To change a preference, click on the Edit link, edit the Current Value and click the Set button.

By default, each user account create expires 1 year form the day it is created. This also applies to the default admin account when its initial password is set.

By default, passwords expire 365 days from when they are set. **Change this if necessary to comply with your organisation's password policy.**

4.2.3   Change Auto-Logoff Timeouts

Session/Auto-logoff timeouts are configured in the *Preferences Manager* which is accessed by navigating to the **Settings > Preference Manager** page.

Set the following preferences to meet your requirements:

- session.timeout.absolute – The number of seconds that a user can be logged in to TsmWeb for at a time.

- session.timeout.idle – The number of seconds that a user can be idle in TsmWeb for, before being logged out.

4.2.4   Disable the default admin account

Prism recommends that once the user accounts have been created, the default TsmWeb *admin* account should be disabled by setting the role for the *admin* account to 'none'.

To do this, create a TsmWeb user account that has the admin role. Login to TsmWeb with this account and change the role of the *admin* user to 'none'.

4.3   Setup PrismToken Users

It is possible to add roles to existing users or create new users and assign roles to those newly created users.

Log into TsmWeb as a user with the 'admin' role (for example, the 'admin' user) and navigate to **Settings > Users** page.

You will require the following users: -

1. A new or existing user account with the 'ptoken-admin' role. Users with this role can administer and operator PrismToken. Administration includes setting preferences, and associating PrismToken with one or more KMCs.

2. For each individual who will operate PrismToken, should have their own user account with the 'ptoken-operator' role. Operation includes getting keys from the KMC and managing Vending Keys.

   a. For each user account the rights should be suitably limited.

   b. For technical operators, the user account permissions should be limited to generation of key change tokens and engineering tokens.

3. Separate user account(s) for testing can be used during development and integration testing. These accounts should be disabled when your PrismToken system is deployed in a live environment.

4. For each client system that will use PrismToken via the Thrift API, a new user account with the 'ptoken-api' role plus one or more 'ptoken-issue-*' roles. For security reasons these accounts should not have any other TsmWeb roles (that would allow them to log in to TsmWeb via the Web Interface).

An example of setting up a new TsmWeb user with the 'admin' role and 'ptoken-admin' role is shown below.

4.4 Preferences

PrismToken preferences can be found in the **Settings > Preference Manager** page that can be accessed from the left navigation bar.

PrismToken preferences contain a "ptoken" prefix.

The default preferences should be suitable for vending.

To issue proprietary engineering tokens (class=2, subclass=11-15) you must set preference 'ptoken.allowIssueProprietaryTokens' to 'true'. The default is 'false', and the user account must have role 'ptoken-issue-any' or both 'ptoken-issue-eng' + 'ptoken-issue-proprietary'.

4.5   Configuring Conductor Service

⚠️ **Please ignore this section if you are using PrismToken as this section is <u>not</u> applicable to HSMs using PrismToken.**

Customers using the low level STS6 API will need to communicate to the STS6 firmware in the HSM via the Conductor service. It is not usually necessary to configure Conductor on the TSM500i-NSS. The default settings will work in most environments. TsmWeb allows the user to manage the Conductor port, the trace level and/or the maximum number of socket connections via the ***Settings > Conductor Settings*** page.

Accessing Conductor from a different subnet through a firewall appliance will require that that the Conductor TCP Port (default 5100) is enabled for incoming connections on the firewall.

4.5.1   Changing the TCP Port

The default TCP Port when the TSM500i-NSS is shipped is 5100. This value may be changed by entering the required TCP Port value and then clicking on `Change Settings` to effect the change.

4.5.2   Trace Level Setting

For normal operation, it is strongly recommended that the **Default** trace level be used. This will log all errors and most warnings. Selecting either of the other two options (Verbose or Debug) will result in **performance degradation** on the TSM500i-NSS due to the additional logging to the embedded storage device. This value may be changed by selecting the required level from the drop down list and then clicking on `Change Settings` to effect the change.

4.5.3   Maximum number of socket connections

The default maximum number of socket connections is 64. This value may be changed by entering the required TCP Port value and then clicking on `Change Settings` to effect the change.

4.5.4   Restarting Conductor

To force Conductor to restart, click the ***Settings > System*** menu and click on `Restart Conductor`. It is not necessary to restart conductor when changing the above settings as this is done automatically.

4.6   PrismToken Dashboard

To access the PrismToken dashboard you will need to be logged in as a PrismToken administrator and click on the "PRISMTOKEN" tab in the left navigation bar.

On the dashboard you will find a "Notices" window. You will need to attend to all of the notices that you may have.
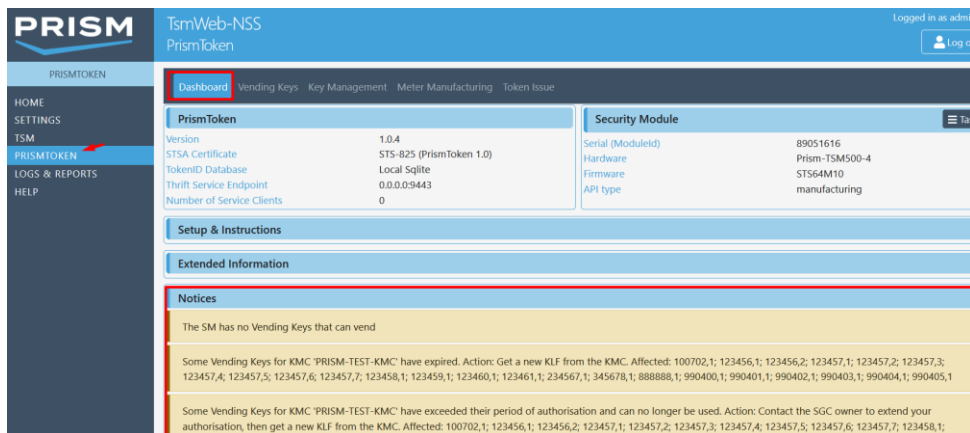
4.7 Backup NSS Settings

The TSM500i-NSS supports a backup of NSS data store and log files to USB flash drive. Data that can be backed up includes network settings, conductor settings, user configuration and preferences. Backup is done using the LCD MAIN MENU on the front panel of the TSM500i-NSS.

- Power the TSM500i-NSS off.

- Insert a USB flash drive (NTFS preferred, FAT32 supported) into the USB port on the front panel of the TSM500i-NSS.

- Power it on again and hold down the red × button and green ✓ button on the TSM500i-NSS front panel until the MAIN MENU appears on the LCD display. Refer to section LCD Menu Sequence for a flow chart of the menu functions.

- Scroll down to Backup to USB option on the MAIN MENU and press the green ✓ button to select. Confirm using the left arrow button.

- Once the backup is complete you will be given the option to continue the boot process. Press the green ✓ button to continue.

Special requirement for backing up large databases

The NSS database is backed up to a single file on the USB flash drive. We recommend using a large-capacity USB flash drive with NTFS format.

Drives formatted with FAT32 have a 4Gb file size limit which may cause the backup to fail if the database is large.

If the backup fails due to lack of disk space or file-size limit then the "boot_log.txt" or "tsmweb_startup_log.txt" will contain a message like "backup failed: database or disk is full".

4.8 Upload Transaction License

If "Transactions Left" is 0 or the "Inhibit Vend Date" is in the past' then you will need to load a Transaction License. Contact your vendor to obtain the Transaction License if required. To load the license on the PrismToken Dashboard, in the "Security Module" box, click the "Tasks" menu and select "Load Transaction License". Follow the on-screen instructions. Please note that the TX license is applicable to STS64Vxx firmware only (STS6 vending HSMs).
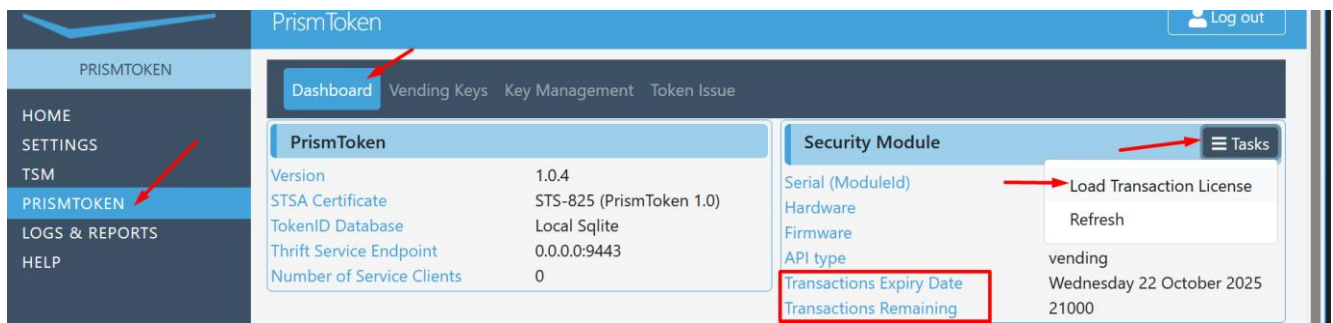
Copy the transaction license certificate (supplied via email by Prism). Include the BEGIN/END lines. Paste it into the "Paste Transaction License" text box below and click the "Load" button.

In this example a transaction license of 1000 with inhibit vend date of 23 October 2025 is applied.
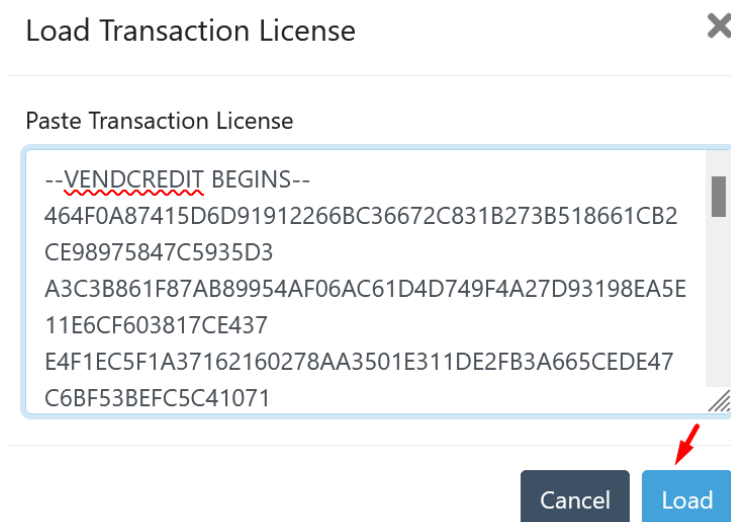
In this example the "Transactions Remaining" increases by 1000 and "Transactions Remaining" changes to 23 October 2025
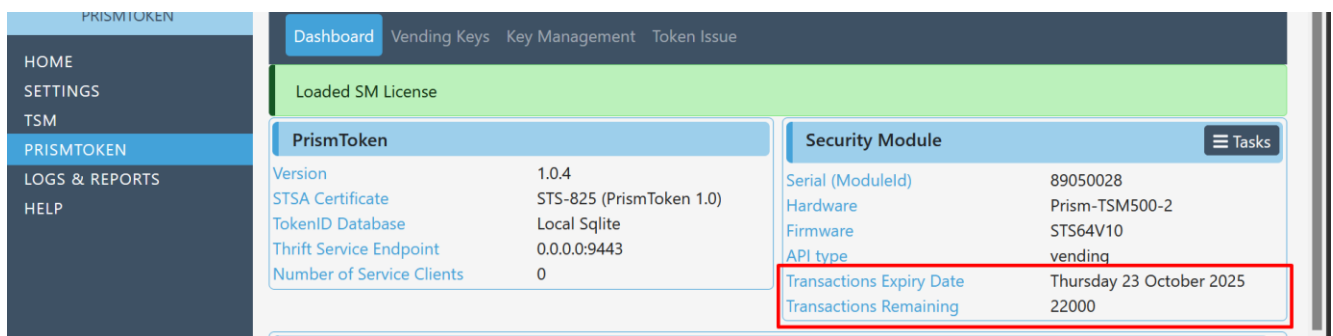
4.9 Upload KMC Public Key

You may need to load one or more KMC PUBKEYs. These keys are required before PrismToken can obtain Vending Keys from the KMC. You must request the KMC PUBKEY from your STS Key Management Centre. For testing purposes, you can find the KMC PUBKEY for Prism's test KMC under the "Documentation" link in TsmWeb's menu.

- Log in to TsmWeb as a PrismToken administrator. Note that a PrismToken administrator will have the role of 'ptoken-admin'.

- Navigate to the **PrismToken** page and click on "Key Management" tab

- Click the "Tasks" dropdown at the top of the tab and select "Upload public key".
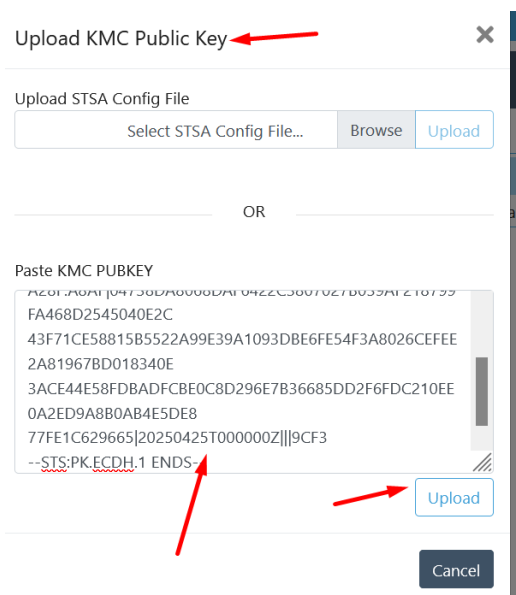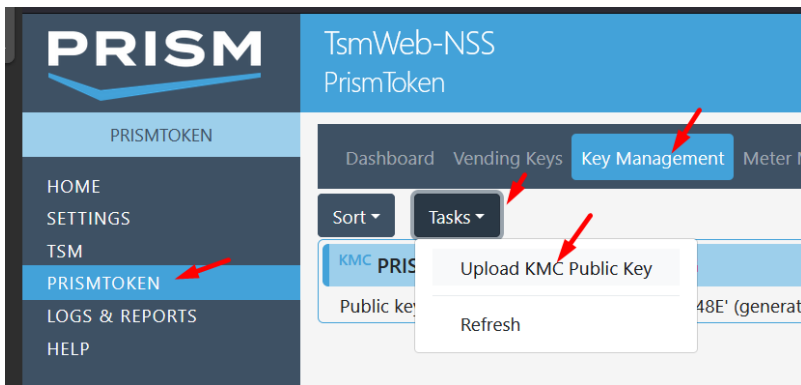
- Open/view the PUBLIC KEY (plain text file) in a text editor then highlight and copy the entire contents. Include the BEGIN/END lines.

- In the "Upload KMC Public Key" popup, paste the contents in the box labelled "Paste KMC PUBKEY", then click "Upload".

4.10 Vending Keys

4.10.1 Generate VKLOADREQ

In PrismToken, on the Key Management tab you should see a list of known Key Management Centres, if you don't you must load the KMC PUBKEY as explained in the previous step. Choose the KMC from which you need to obtain Vending Keys, click that KMC's "Tasks" menu and choose "Generate VKLOADREQ". Follow the on-screen instructions. You will need to copy & paste the VKLOAREQ into an e-mail and send it to the KMS via email (KMS Operator) for processing.
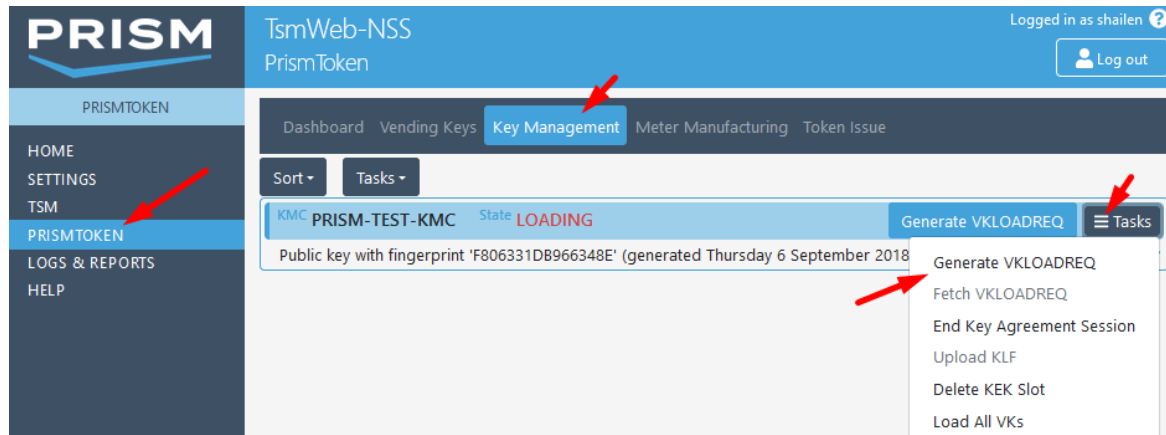
⚠️ **Send the most recent VKLOAD.REQ.1 record to the KMC (not an earlier one). The SM stores the timestamp of the last VKLOADREQ and will not accept a VKLOADRSPKMC unless it matches that timestamp.**

4.10.2 Upload KLF into PrismToken

The KMC will reply with an e-mail that has a Key Load File attached. To upload the Key Load File go to PrismToken, click on "Key Management" tab, the KMC's "Tasks" menu, and choose "Upload KLF". You can then navigate to PrismToken's "Vending Keys" tab where you will see your vending keys. **At this point the vending keys are uploaded into PrismToken and have not been loaded in the security module as yet.**

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

⚠️ **The security module stores the timestamp of the last VKLOADREQ and will not accept a VKLOADRSP_{KMC} unless it matches that timestamp. NOTE: Sometimes users commit the mistake of generating another VKLOADREQ after submitting a current VKLOADREQ to the KMC! In such a scenario the following error will be returned by the SM for an SM?KR request: SM!KREEPSM.3B.8: Bad VKLOADRESP: wrong timestamp (TVP) in VKLOADRESP_KMC; possible expired or out-of-order response~AF0A.**

4.10.3 Load All Vending Keys

Uploading the KLF loads the information from the KLF into PrismToken and it passes the VKLOADRSP to the security module. PrismToken does not load any of the keys from the KLF into the security module. When the security module processes the VKLOADRSP the vending keys for that KEK slot are erased from the security module.

To load the keys from the KLF you will need to select the "Load All VKs" option from the "Tasks" menu. Take note that if the key agreement session is ended before loading all the vending keys, then it will not be possible to load vending keys from the same KLF file into the security module. A new VKLOADREQ will need to be generated and sent to the KMS via email (KMS Operator) for processing. The KLF returned from the KMS needs to be uploaded and then you will need to select the "Load All VKs" option from the "Tasks" menu. Refer to Section 4.10.4 if "Load All VKs" returns the following error Failed to load all VKs: STS API error VK_REG_NOT_FOUND_ERROR (code 28)

4.10.4 Load Individual Vending Keys

There may be circumstances where the number of vending keys within a security module's KLF exceeds the maximum number of vending key registers available in the security module. This is a hardware limit based on the TSM family. A TSM250 has a limit of 25 key registers/slots whereas the TSM500i supports up to 999. Exceeding this limit is often due to TSM250 customers requesting far too many of the manufacturer default SGC's. In practical terms, very few of these default SGC's are required. The STSA have introduced two universal default Supply Group Codes (SGC) which are available to anyone:

- 1993 Base Date Universal Default 991993
- 2014 Base Date Universal Default 999014
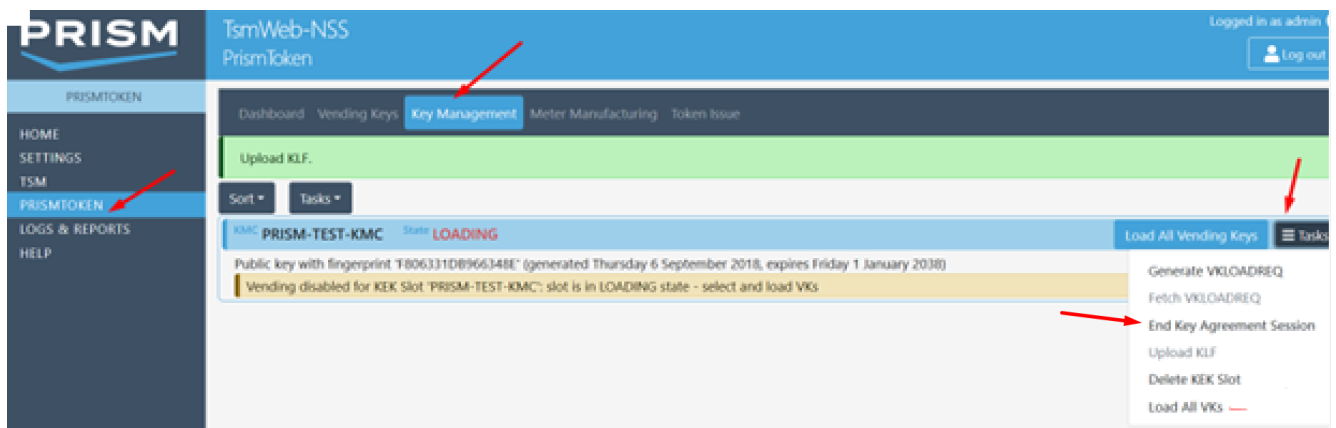
After uploading the KLF on the Key Management tab, instead of using the "Load all Vending Keys" button, navigate to the Vending Keys tab and change the "Filter" to show all vending keys and not just those in the security module.
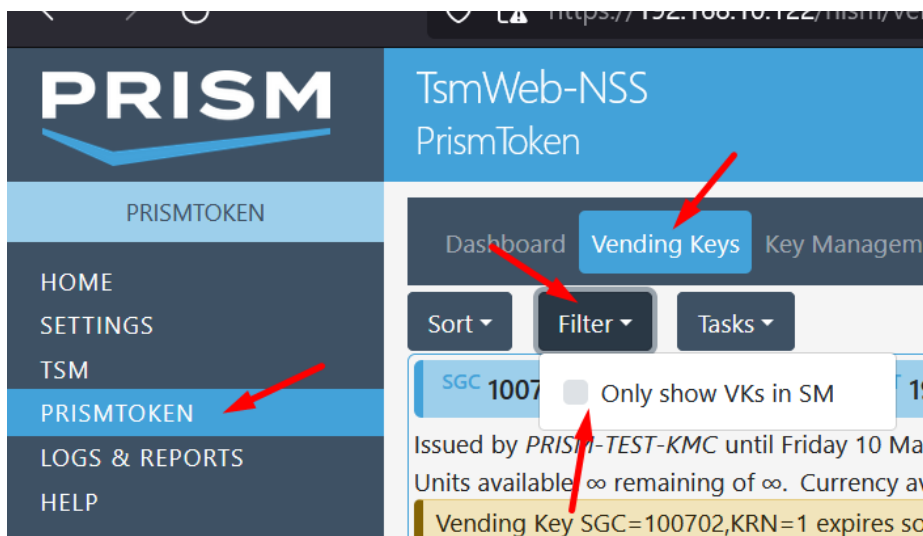
There is a task button per vending key, where there are two options. You can load or delete the vending key from the security module.
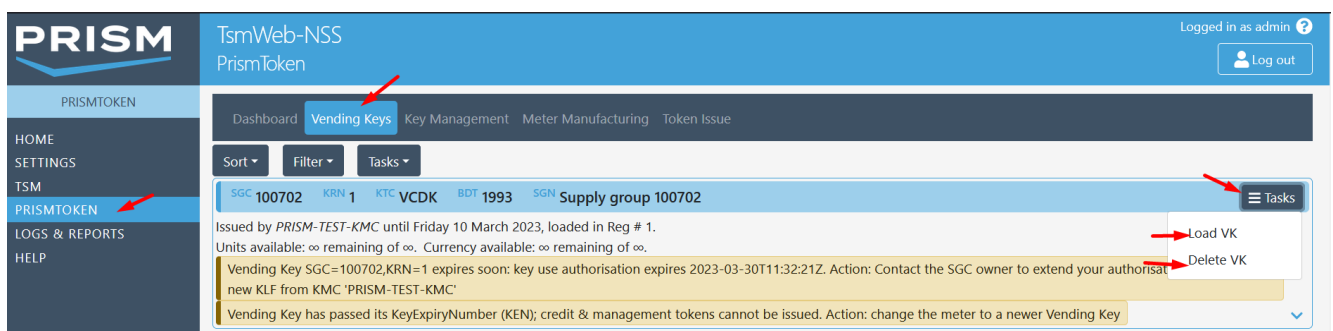
With vending firmware when the KEK Slot is in "Loading" state it is not possible to use the STS Vending commands. The key agreement session must be closed by selecting End Key Agreement Session which results in the KEK slot moving to the "Active" state which allows the STS Vending commands to be used.

5 Configure and Test Access Service

5.1 PrismToken Thrift API

5.1.1 Automating PrismToken using the Thrift API

PrismToken has a remotely callable Thrift API that can be used to integrate its token issue capabilities into your applications. See the documents PR-D2-0984 "Guide to Using Thrift" and PR-D2-1009 "PrismToken Thrift API" to learn more about Thrift and the API. Client code for the Thrift API is generated using the open source software "Apache Thrift" and the API definition file "prismtoken1-TokenApi.thrift" which you will find under TsmWeb Documentation. We can supply pre-built client code with examples for the C#, Java, and PHP languages. If you are using another language, please contact us for advice. The PrismToken Thrift API service is accessible at your NSS's IP address, on port 9443 by default (you can check the port number on the PrismToken dashboard). A client must authenticate itself by calling the signInWithPassword() method using realm="local" and the credentials of a TsmWeb user account that has 'ptoken-api' role (plus 'ptoken-issue-*' roles as required).

5.1.2 Generating STS Tokens by integrating with the thrift API

- In a typical STS deployment, a Vending System would manage a database of meters with associated point of connection, tariff, customer, etc. The Vending System would integrate with PrismToken to generate tokens (much like legacy Vending Systems integrate with the TSM210 or TSM410 Security Module).

- The documents "Guide to Using Thrift" and "PrismToken Thrift API" (both attached) explain the Thrift protocol and the functions available in the PrismToken API (which is accessed using the Thrift protocol).

- You will need to develop client software that calls the PrismToken Thrift API to generate the Key Change Tokens and Credit Tokens as they are needed by the Vending System.

    a) Your client software will call the issueCreditToken() function to issue a Credit token (optionally with Key Change Tokens to update the meter to the latest KRN).

    b) Your client software may also call the issueKeyChangeTokens() function to issue Key Change Tokens explicitly.

- Below is a code snippet that comes from the Java development pack for PrismToken and is a simple example of how client software uses the Thrift library to call PrismToken.

- Currently PrismToken has development packs for C#, Java and PHP. Other language libraries can be made available on request.

```java
package za.co.prism;
import za.co.prism.prismtoken1.*;

public class PrismTokenClient {

  public static void main(String [] args) throws Exception {
    // Connection options
    String host = "196.214.189.218";
    int port = 9443;
    String username = "ptapiuser";
    String password = "Ptapiuser1";

    // Create a PrismToken Thrift client
    // Note 1: The Prism NSS does not know its DNS name and the certificate is self-signed,
    //    so cannot use Thrift's TSSLTransportFactory but must reproduce its logic with
    //    a tailored SSL connection that permits the untrusted certificate and hostname mismatch.
    //    In a production environment you should add the NSS certificate to your trusted store.
    System.out.print("\nConnecting to host='" + host + "' port='" + port + "'\n");
    javax.net.ssl.SSLContext ctx = javax.net.ssl.SSLContext.getInstance("TLS");
    ctx.init(null, trustAllCerts, new java.security.SecureRandom());
    // HostnameVerifier only required for HTTPS, not Thrift/TLS
    javax.net.ssl.SSLSocket socket = (javax.net.ssl.SSLSocket) ctx.getSocketFactory().createSocket(host, port);
    socket.setSoTimeout(0);
    org.apache.thrift.transport.TTransport trans = new org.apache.thrift.transport.TSocket(socket);
    trans = new org.apache.thrift.transport.TFramedTransport(trans);
    System.out.print("-> Connected\n");
    org.apache.thrift.protocol.TProtocol proto = new org.apache.thrift.protocol.TBinaryProtocol(trans);
    TokenApi.Client ptoken = new TokenApi.Client(proto);
    System.out.print("-> PrismToken client created\n");

    // Basic comms test
    System.out.print("\nPrismToken Ping()\n");
    String pingResp = ptoken.ping(0, "Hello, world!");
    System.out.print("-> " + pingResp + "\n");

    // Sign in
    System.out.print("\nPrismToken SignInWithPassword()\n");
    SignInResult result1 = ptoken.signInWithPassword(java.util.UUID.randomUUID().toString(),
      "local", username, password, new SessionOptions());
    String accessToken = result1.getAccessToken();
    System.out.print("-> OK\n");

    // Issue a 100kW Electricity token to a meter
    System.out.print("\nPrismToken IssueCreditToken()\n");
    MeterConfigIn meter = new MeterConfigIn(/*drn*/ "00000000000", /*ea*/ (short)7, /*tct*/ (short)1,
      /*sgc*/ 123456, /*krn*/ (short)1, /*ti*/ (short)1, /*ken*/ (short)255);
    meter.setAllowKrnUpdate(false);
    java.util.List<Token> result2 = ptoken.issueCreditToken(java.util.UUID.randomUUID().toString(),
      accessToken, meter, (short)0, 100.0 * 10, 0, 0);
    java.util.Iterator iter2 = result2.iterator();
    while (iter2.hasNext())
    {
      Token t = (Token)iter2.next();
      System.out.print("-> " + t.toString() + "\n");
    }

    // Done
    System.out.print("\nDone\n");

    trans.close();
  }

  // See e.g. https://nakov.com/blog/2009/07/16/disable-certificate-validation-in-java-ssl-connections/
  static javax.net.ssl.TrustManager[] trustAllCerts = new javax.net.ssl.TrustManager[] {
    new javax.net.ssl.X509TrustManager() {
      public java.security.cert.X509Certificate[] getAcceptedIssuers() {
        return null;
      }
      public void checkClientTrusted(java.security.cert.X509Certificate[] certs, String authType) {
      }
      public void checkServerTrusted(java.security.cert.X509Certificate[] certs, String authType) {
      }
    }
  };
}
```

5.2 Conductor

If PrismToken is not being used then client software must be configured to communicate with TSM500i HSM Conductor service, and then tested to ensure that transaction processing can proceed successfully.

Such configuration and testing will make use of third-party tools that are beyond the scope of this guide. Consult the software documentation or contact your application vendor for assistance.

6 Security, Operations, and Monitoring

This section provides guidance for operating PrismToken securely and reliably in a Live environment.

6.1 General

General guidance for Live environments:

- IT equipment can fail unexpectedly. You should always have a Disaster Recovery (DR) plan. That plan should include a standby PrismToken and Security Module, fully loaded with Vending Keys, and monitored regularly to ensure that the standby system is functional (with non-expired keys!). You will also need to plan how to fail over to the standby system.

6.2 Security in a Live Environment

- Do not expose PrismToken, TsmWeb, or the NSS to the Internet. Deploy PrismToken on a network segment that is firewalled from inbound Internet traffic. Use a packet filter or VPNs/tunnels to restrict access to only those clients/networks that need it.

- Follow the relevant setup guides for the NSS, TsmWeb, and the Security Module.

    o Once the administrator password is set the NSS is secure-by-default and no additional security configuration is required for a Live environment.

- Authentication to PrismToken and/or TsmWeb is by username and password. Use strong passwords on all accounts. Restrict accounts to the minimum roles required to fulfil the account's purpose. Disable unused accounts.

- Client software that integrates with the PrismToken API should verify the TLS certificate of the server (i.e. TsmWeb/PrismToken). You can obtain the TLS certificate from the Network page in TsmWeb, by using the "Tasks" button of the "SSL/TLS Server Properties" section; alternatively you can query the TLS certificate using a tool like openssl. Client authentication by means of client-side certificate is not supported.

    o Procedures for converting the certificate format (if necessary) and importing it into your client's trusted store vary by client, development language, and operating environment, and are beyond the scope of this document. Your client software should document the steps required.

6.3 Vending Key Settings at the KMC

Various Vending Key attributes that are set at the KMC can influence your operational environment. If you own the Supply Group then you have control over these attributes.

- The Vending Key's Refresh Period determines how frequently keys must be refreshed, i.e. how frequently you must get a fresh Key Load File (KLF) from the KMC. On PrismToken the Vending Key's "IUT" (Issued Until) attribute indicates when the current issue will expire and prevent the key from being used. The IUT may be different for every Vending Key.

- The Vending Key's Key Expiry Number (KEN) and Expiry (EXP) determine when the Vending Key expires and *will no longer be issued by the KMC or allowed to be used in any Security Module*. The KEN and EXP

are usually set to a far-future date, but in some cases (such as a compromised key) these dates may be brought forward to force a key change on all meters.

- The Vending Key's Subclass Bitmap (SBM) can restrict which resource subclasses (Electricity, Water, Gas, Time, Currency) are allowed in a Credit vend. SBM is usually set to 0x00FF or 0xFFFF to allow all subclasses.

6.4   PrismToken Setup

The following settings can be accessed through the Preference Manager, and can help you monitor PrismToken:

- If you use PrismToken in Meter Manufacturing then ensure that *ptoken.meterManufacturingMode* is set.

- If you use PrismToken in Vending and need to issue proprietary Manufacturer tokens, then ensure that *ptoken.allowIssueProprietaryTokens* is set.

- Setting *ptoken.sessionTimeoutSec* determines the duration (in seconds) of an authentication session with the PrismToken API. The client must re-authenticate when the session expires. Your client software should document an appropriate range for this setting. The default is 300 second, which we believe is a good trade-off between security and usability. We recommend against values outside the range 120-86400.

- Settings *ptoken.inhibitVendWarningDays* and *ptoken.txCounterLowThreshold* cause SM License warnings on the PrismToken dashboard when these thresholds are crossed.

- Settings *ptoken.keyExpiryWarningDays* and *ptoken.keyRefreshWarningDays* cause Vending Key Expiry warnings on the PrismToken dashboard when these thresholds are crossed.

- Setting *account.password.maximum.age.days* determines the maximum age of a password. An account password must be changed within this period, or the account will be locked out (requiring administrator intervention).

6.5   Monitoring

Reliable operation requires regular monitoring. We recommend the following checks on a regular schedule (at minimum once per week):

- On the TsmWeb Licenses page check the "Expires" date under "NSS License". If the license will expire soon contact Prism to renew your license.

- On the TsmWeb Network page check the "Certificate Expires" under "SSL/TLS Server Properties". If the certificate will expire soon use the "Tasks" menu to "Generate new TLS key and certificate". The TsmWeb home page will show a warning if the certificate will expire within 30 days.

    o After generating a new certificate, you will need to add the new certificate to the trusted stores of your clients, as explained in 6.2 above.

- Check for alerts on the TsmWeb Alerts page.

- Check for Notices on the PrismToken dashboard. First click "Tasks" -> "Refresh" to ensure you are viewing current (not cached) information. These notices will alert you of current or pending problems with PrismToken, including:

o The Security Module "Inhibit Vend Date" (visible in the "Security Module" section of the PrismToken dashboard) is within *ptoken.inhibitVendWarningDays*. Contact Prism to update your license.

o The Security Module's "Transactions Left" (visible in the "Security Module" section of the PrismToken dashboard) is below *ptoken.txCounterLowThreshold*. Contact Prism to update your license.

o One or more Vending Keys has an Issued Until (IUT) date within *ptoken.keyRefreshWarningDays*. You will need to obtain a fresh Key Load File (KLF) from the KMC.

o One or more Vending Keys has an Expiry (EXP) or Key Expiry Number (KEN) date within *ptoken.keyExpiryWarningDays*. This could be because the Vending Key is being phased out, or the Supply Group owner no longer wants you to have the key. You will need to consider the impact of this key expiry on your vending environment, and contact the Supply Group owner(s) of the affected Vending Key(s) if these values needs to be changed.

o One or more Vending Keys cannot vend (attribute VND=0) for a reason not related to SM License or IUT/EXP. This typically happens when the Unit Limit or Currency Limit of the Vending Key has been reached (described in more detail below). If you see a warning that keys cannot vend then you will need to inspect each key on the PrismToken Vending Keys page, identify the key(s) with VND=0, and determine the reason for each.

o Real-time clock drift exceeds *ptoken.rtcDriftHighThreshold*. The Security Module enforces STS rules that require the token timestamp to be within a narrow window of real (wall-clock) time. If the Security Module's internal clock is very different from the clock of the NSS (or PC) this may prevent tokens from being issued. The resolution is typically to synchronise the time of the NSS (or PC) to the SM's clock (the NSS normally does this automatically). If the SM's clock is very different to wall-clock UTC time (more than 24 hours) then contact Prism for advice.

- On the PrismToken Key Management page:

o For Vending (not Manufacturing) systems: Check that none of the KMC cards are in LOADING state. Vending Keys associated with that KMC cannot be used in vending operations when the KMC card is in LOADING state. The card should only be in LOADING state if a Key Load File has been uploaded but the loading session has not been completed (by loading VKs and ending the key agreement session).

o Check the "expires" date of the "Public key" of each KMC. If the key is expired (or will expire soon) then you should contact the KMC for an updated Public key. You need an active (not-expired) Public key to generate a VKLOADREQ and thus to get a fresh Key Load File from the KMC.

- On the PrismToken Vending Keys page:

o If you have any Vending Keys with a Unit Limit (ULM) or Currency Limit (CLM), then check these values to ensure that they are not close to zero. These financial risk control values limit the amount of Credit Units or Credit Currency that can be issued by the Security Module using that Vending Key. They are set to a maximum (determined by the Supply Group owner at the KMC) when the keys are refresh by loading a Key Load File, then decremented whenever a Credit token is issued. When they reach zero you will not be able to issue further credit tokens. If these values are low, you will need to obtain a fresh Key Load File (KLF) from the KMC.

- On the TsmWeb Users page check the "Accounts expires" and "Password expires" of every account. You can extend the account expiry date by editing the account. To extend the password expiry date

you must set a new password (humans users should be instructed to change their own passwords; for API client software you will need to distribute the new password to the client).

- Check the TsmWeb Activity page. If these is lots of activity from User=$ANON, from IP addresses not on your network, or the Activity looks suspicious, then your TsmWeb/NSS may have been scanned by a vulnerability scanner. Check with your IT department whether this was an intentional security activity undertaken by them; if not then: (1) investigate whether the IP addresses indicate an internal or external scan; (2) for external scan revise your firewall rules to prevent direct access to TsmWeb/NSS; (3) for internal scan hand to your IT security team for investigation.

- On the TsmWeb home page check the "Disk Space". If less than 100Mb is available, then old data needs to be trimmed from the database. Database trimming is performed automatically by TsmWeb versions 4.70 and higher.

6.6 Known issues affecting reliability

The following activities are known to potentially affect reliability of PrismToken:

- TsmWeb UI operators should avoid time-consuming operators such as report generation. Such operations can block out all PrismToken API calls until completed.

- Ensure that PrismToken is not overloaded by API calls. If you see a consistent increase in call latency this could indicate that you are at PrismToken's maximum performance.

- We have a few reports of an intermittent problem when loading a Key Load File that can put the SM into LOADING state but without Vending Keys available to load. This is potentially serious in a Live environment and may require fail-over to a standby/DR system. We are investigating the problem but have been unable to reproduce it.

- The NSS is an embedded system with limited resources, and various internal protections against malicious modification that can progressively consume these resources when the NSS is under load for extended periods (as would be expected in a Live environment), potentially resulting in a system freeze. To ensure reliable operation we suggest a scheduled reboot of the NSS approximately once per week at an off-peak time. We are investigating resolutions for this problem.

7 Status & Diagnostics

7.1 TSM500i Status Information

The user can view the current status of the HSM as well as the history of security-related events on the HSM.

Select the **TSM > TSM Status** to obtain a report with detailed status information. The status information displayed will differ depending on whether you are in the **Loader** state or the **Operational** state.

If in the **Loader** state, the following information will be displayed: UID (unique identifier), Boot Loader version, firmware type and version, current access control mode, firmware key identifiers, active and latched tamper conditions (if applicable), module current date & time, and firmware license. In addition to the above, the status report also provides an Audit Log containing all module Bootloader Audit Log entries. This audit log gives the date and time of events such as hardware resets, operator logins, tamper events (occurrence and clearing thereof), loading of firmware, resetting or changing of passwords, and other security-related information.

If in the **Operational** state, the following information will be displayed: UID (unique identifier), firmware type and version, current access control mode, SMK details. The status report also provides an Audit Log containing all Application firmware audit log entries in addition to the Boot Loader audit log entries described in the previous paragraph.

7.2 NSS Log Files

To access NSS log files select the **Logs & Reports > Log Files** page from the side menu. The following types of logs are available:

- boot: contains TSM500i-NSS boot and TsmWeb start-up logs

- conductor: contains Conductor logs which apply to the MCM API

- nss: contains TsmWeb and x-comsvcio (which apply to the Common API) logs

- tsm500drv: contains tsm500drv logs

In addition to these log files TsmWeb also logs all web browser interaction from users in its database. This activity can be viewed in various reports which can be accessed via the **Logs & Reports > Reports** page from the side menu.

7.3 Network Diagnostics

To communicate with the TSM500i-NSS HSM both the computer and the HSM initially both need to be on the same subnet.

If the HSM is being access from a different subnet, then the NSS default gateway needs to be set so that network packets can be routed via the default gateway to your computer.

Tools that can be used to test connectivity are:

- **ping** - command line to that can be run from the command prompt. The TSM500i-NSS responds to ping, but firewalls or gateways between the client computer (where you are running ping) and the TSM500i-NSS may block pin packets.

- **PowerShell Test-NetConnection** - Tests that a TCP connection can be made to the service's port on the NSS. Do this from the PC where the client software (that uses the NSS) will run. Look on the Networks page to get the port. Connection may fail if there is a routing problem between the client computer & TSM500i-NSS, or if the communication is blocked by a firewall or gateway.

  Example usage: Test-NetConnection -ComputerName 192.168.0.130 -Port 5100

7.4 Network Diagnostics (NSS service/firewall specific)

The TSM500i-NSS has a firewall. It opens the firewall for the listed ports on the Network page. You must ensure that any firewalls between the client PC and the NSS must allow the traffic to services required by the client computer. When setting up network access for TsmWeb any firewalls or gateways between computer and the HSM need to allow network traffic on TCP port 80 and 443.

When setting up network access for Conductor (MCM API) any firewalls or gateways between computer and the HSM need to allow network traffic on TCP port 5100 (default) or the specific port setting being used for Conductor.

When setting up network access for HSM Server (Common API) any firewalls or gateways between computer and the HSM need to allow network traffic on TCP port 1500 (default) or the specific port setting being used for Conductor.

7.5 Look at the LCD

If you cannot communicate with TsmWeb, Conductor or the HSM Server waiting for the TSM500i-NSS to boot up then have a look at the LCD on the front the HSM. There could be useful diagnostic information than can be supplied to Prism who can advise what should be done next to resolve the issue.

7.6 TSM500i Status LEDs

After powering on the TSM500i-NSS check status LEDs that are located on the front panel. Refer to section 3.2 for description of the LED states.

7.7 Contact Prism Support

To provide support Prism will require log files, and to know what you have already tried.

There are two ways to get logs from the TSM500i-NSS:

- If you have access to TsmWeb navigate to *Logs & Reports > Log Files*, then click on the **Download all logs as ZIP** button.

- Logs are written to a USB flash drive when the TSM500i-NSS boots. The flash driver should be inserted into the USB port before powering on the TSM500i-NSS.

8 Managing TsmWeb

8.1 SSL/TLS Certificate

TsmWeb uses TLS by default to secure browser connections. The login page, and all pages that require the user to be logged in, are only accessible using TLS. TLS can be disabled but this is not recommended.

When TsmWeb generates a certificate, it assigns it a validity period of 398 days. The **Home** page and **Settings > Network** page displays the TLS certificate expiry date.

The TsmWeb alert system is used to notify the user that the certificate is going to expire when the expiry date reaches the notification window of 90 days remaining. Each time a session is established a warning will be generated which can be acknowledged from within TsmWeb.

Steps to Generate a New TLS Key and Certificate:

A new certificate and key pair can be generated via the **Settings > Network** page. To do so, click on the ☰ TASKS button on the "SSL/TLS Server Properties" pane, and then select "Generate new TLS key and certificate". The TSM500i-NSS will need to be rebooted so that the new certificate can take effect.

The TLS key algorithm can be changed by changing the *tls.key_data* preference value via the **Settings > Preferences Manager**. Both RSA and EC key types are supported.

As a fail-safe mechanism, if a new certificate has not been generated before the current certificate expires; the server will automatically generate a new certificate on start-up. If a user is unable to connect due to the certificate having expired, the TSM500i-NSS will need to be rebooted so that the new certificate can take effect.

8.1.1 SSL / TLS can be disabled (Not Recommended)

⚠️ TLS is a PCI-DSS security requirement applicable to payments and many other environments. This service should NOT be disabled except as a temporary measure to resolve a specific TLS-related problem.

8.1.1.1 *Disable or Enable TLS from TsmWeb*

To enable or disable TLS via TsmWeb, navigate to **Settings > Preference Manager** and edit the *tls.enabled* preference as required.

After enabling or disabling TLS from TsmWeb, it will be necessary to power-cycle the TSM500i-NSS in order for the new setting to take effect.

8.2 Preference Manager

TsmWeb can be configured using various preferences. Preference values can be viewed and updated using the ***Settings > Preference Manager*** page. This page displays a table of preferences and their associated values.

A user can change a preference value if an "Edit" link is shown in the corresponding table row. Note that a user may not be able to edit a preference due to having insufficient user permissions, or the preference being read-only. Any preferences that have been changed from their default values will be indicated as such in the status column.

Note that the preferences on this page are TsmWeb settings and are not stored on the HSM. When a backup to USB is done (see section 4.4) all the preferences are included in the backup.

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

9 Managing Your NSS

9.1 NSS LCD Menu

The LCD's MAIN MENU allows the following settings to be modified: IP Address, Netmask, default gateway, USB Backup & Restore, Disable SSL/TLS and Resetting of parameters such as Admin Password and factory default settings.

The LCD Main Menu on the TSM500i-NSS may be accessed by powering the TSM500i-NSS off and then on again. Watch the LCD display and, when prompted, press and hold down the red **✗** button and green ✓ button on the front panel until a MAIN MENU appears on the LCD display. The arrow keys may be used to select the required option.

For details on how to navigate and use the MAIN MENU, refer to section 3.3.1 or LCD Menu Sequence.

⚠️ Resetting any of the TSM500i-NSS settings described here has NO effect on the TSM500i Hardware Security Module (HSM). Refer to the block diagram in Section 1.1 to see how the HSM is physically separated from the embedded computer system.

⚠️ No keys or Crypto Officer passwords that are stored inside the TSM500i HSM will be lost when performing the procedures detailed in this section.

The settings that may be changed are:

- Admin Password Reset   - refer to section 9.3.1
- Set IP Address, Netmask, default gateway   - refer to section 3.3.1
- USB Backup & Restore   - refer to section 4.7
- Reset to Defaults   - refer to section 9.3
- Disable SSL/TLS, reset TLS key   - refer to section 9.4

9.2 Backup and Restore

9.2.1 Backup & Restore on a TSM500i-NSS

Backup

Refer to section 4.7 for the procedure to backup NSS settings and the TsmWeb database to a directory "NSS_BACKUPS" on the root of a flash drive.

Restore

A USB flash drive that has the "NSS_BACKUPS" directory from a previous backup operation is required for a restore.

- *An NSS backup must be restored to an NSS with the same (or higher) firmware version.*

- Switch the TSM500i-NSS off.

- The flash drive should be plugged into the USB *Service* port on the front panel.

- Power it on again and hold down the green ✓ button and red ✗ button on the TSM500i-NSS front panel until the MAIN MENU appears on the LCD display. Refer to LCD Menu Sequence for a flow chart of the menu functions. This takes approximately 20 seconds.

- Scroll down to USB Restore option on the MAIN MENU and press the green ✓ button to select. Confirm using the left arrow button. The message 'NSS Restore' is displayed followed by NSS Restore – Success.

- Wait for the Main Menu to appear on the LCD. Select Continue Reboot.

Additional considerations for restoring a backup to a different NSS

You can use Backup & Restore to migrate your settings and data from one NSS to another, but take note of the following:

- *An NSS backup must be restored to an NSS with the same (or higher) firmware version.*

- Network settings are restored, so the restored NSS will have the same IP address as the backed up NSS. When restoring to a different NSS you should physically disconnect the NSS from the network before restoring; then use the NSS LCD Menu (0) to change the network settings after restoring; then reconnect the NSS to the network.

Special requirement: restoring a backup from NSS v4.57 or before

From NSS v4.58 onwards backups are made to a folder "NSS_BACKUPS\tsmweb_db_backup".

Before NSS v4.58 backups were made to a single file "NSS_BACKUPS\tsmweb_db_backup".

To restore a backup taken on NSS v4.57 or lower, to an NSS with v4.58 or higher, you must rename the file "NSS_BACKUPS\tsmweb_db_backup" to "tsmweb.sqlite", and then move it to the subfolder "tsmweb_db_backup", so that your backup contains the single file "NSS_BACKUPS\tsmweb_db_backup\tsmweb.sqlite".

If you do not make this manual change to the backup, the "boot_log.txt" or "tsmweb_startup_log.txt" will contain an error like "source directory, 'E:/NSS_BACKUPS/tsmweb_db_backup', is not accessible".

Special requirement: restoring a backup from NSS v4.75 or before

NSS v4.75 introduces a new database structure that improves disk space utilization.

To restore a backup taken on NSS v4.74 or lower, to an NSS with v4.75 or higher, the restore operation requires free space on the USB flash drive (that contains the backup) to perform a database migration. The USB drive must have free space equal to THREE (3) times the size of the largest file in the "NSS_BACKUPS\tsmweb_db_backup" folder. The database migration may take several minutes with a small database, up to several hours for a multi-Gigabyte database.

9.3   Reset NSS to Default Settings

Section 9.1 details how to access the Reset submenu from the NSS LCD Main Menu. The Reset Menu includes a number of options and the associated default values are detailed below:

9.3.1   Admin Password Reset

In the event that the password has been lost, you will require access to the TSM500i-NSS front panel. Perform the following procedure:

Power the TSM500i-NSS off and then power it on again. Watch the LCD display and, when prompted, press and hold down the red ✖ button and green ✓ button on the front panel until a MAIN MENU appears on the LCD display. Use the arrow keys to select the ***Reset...*** option. Press the green accept key and then select the ***Admin passwd*** option. After confirming, wait until the LCD display returns to the MAIN MENU and then press the green accept key to continue booting.

Once the TSM500i-NSS has powered up, a new admin password for TsmWeb may be set in accordance with section 3.4.2.1.

Select the "Admin Passwd" option to ERASE the current Admin Password. Once this has been done a new Admin Password may be set as described in section 3.4.2.1.

9.3.2   Config Reset

Selecting the "Config reset" option from the *RESET MENU* will reset in ALL user-configured settings being reset to their default values. This includes the following:

IP address	(reset to 192.168.0.201)
net mask	(reset to 255.255.255.0)
default gateway	(reset to "none")
TCP Port	(reset to 5100)
Trace level	(reset to "default")

9.3.3   Factory Reset

The "Factory Reset" option is only available to the HSM Manufacturer and is used to deleting all database files including the logs, as well as the settings that are reset by "Config reset".

9.4   Disable TLS from the LCD MENU

Using the LCD MAIN MENU as described in section 9.1, select the "Disable TLS" option and confirm the operation. The TLS service is now disabled.

9.5 Upgrading TSM500i-NSS System Software

ⓘ **Upgrading the TSM500i-NSS System Software is distinct from TSM500i HSM application firmware should not be confused with upgrading the TSM500i HSM Application Firmware.**

The TSM500i-NSS consists of a TSM500i hardware security module that interfaces to an embedded computer system (refer to the block diagram in Section 1.1). The embedded computer system has its own operating system and, amongst other things, runs the Conductor service and provides the TsmWeb interface.

It may be necessary from time to time to provide an update to one or more of the software components that run on the TSM500i-NSS embedded computer.

9.5.1 Software upgrade via USB service port

If you receive an NSS software upgrade from Prism the mechanism for these software updates is via the USB *Service* port on the front panel of the TSM500i-NSS. The procedure to upgrade is as follows:

- *We strongly recommend performing a backup before any upgrade.*
- Copy the upgrade files the NSS_UPDATES directory to the root path of a USB flash drive
- Power the TSM500i-NSS **off**
- Insert the USB flash drive into the *Service* port
- Power the TSM500i-NSS **on**
- Observe the LCD on the front panel of the TSM500i-NSS. The LCD will display a prompt asking whether the updates should be applied. Press the green ✓ button on the front panel.
- Wait until the update process completes, no further user intervention is required
- The NSS will automatically execute any required reboots in order to complete its updating

When the system software upgrade is completed, the LCD will display "TSM500-NSS READY". The revision of the system software is reported during the boot cycle.

Special requirement: upgrading from versions before NSS v4.75

NSS v4.75 introduces a new database structure that improves disk space utilization. The process of upgrading to v4.75 (or higher) includes a mandatory and automatic backup, plus a database migration (that is performed via an automatic restore). The USB flash drive that contains the NSS_UPDATES directory must have free space equal to FOUR (4) times the size of the NSS database, or the upgrade will fail. You may need to take a backup to discover the size of the database. The upgrade process may take several minutes with a small database, up to several hours for a multi-Gigabyte database. We strongly recommend using a USB flash drive with NTFS format.

9.5.2   Remote software upgrade via TsmWeb

ⓘ   **From NSS v5.20 s/w onwards updates can be performed REMOTELY via TsmWeb. It will be possible to update NSS Software WITHOUT being physically at the HSM provided that update 5.20 has previously been applied using a USB stick at the HSM.**

⚠️   A TSM500i-NSS that was manufactured BEFORE July 2018 will NOT be able to support REMOTE updates of NSS software. Upgrades must continue using USB.

If your TsmWeb menu does NOT have a **SETTINGS > UPDATE NSS** page, then remote updates are NOT supported (this will typically be on any TSM500-NSS where the ID reported in the bottom status bar of TsmWeb starts with "TSM500-...").

Web interface	
Web UI port	443 (80)
Web service port	8080

Generated at 2023-08-04 13:33:20 by **Prism TsmWeb-TEST-KMS v4.85.3** in 161.769ms or TSM500-DN09WD7Y.

Download latest ZIP file from the FTP server e.g. NSS_v5.XX_UPDATE_REMOTE(includes xxxxx).zip. Do NOT unzip this file.

Upload and apply the update using TsmWeb from the "UPDATE NSS" menu option under "SETTINGS".

9.6   Configuring SNMP

Refer to TSM500i-NSS SNMP Application Note (PR-D2-1121) for instructions on how to enable SNMP in TsmWeb.

9.7 LCD Menu Sequence

Flow diagram with LCD display annotations:

- **Power on NSS** → `TSM500-NSS BOOT` / `Start OS`
- **NSS-INIT process starts running** → `NSS 4.70 BOOT` / `Start INIT...`
- **Detect USB disk inserted** — NO / YES
- **Apply upgrade and reboot**
- **Detect if USB contains relevant upgrades** — YES → **Apply available upgrades?** → `Update NSS` / `Software? ✓Y N✗`
  - YES (✓) → Apply upgrade and reboot
  - NO (✗)
- **NSS-INIT calls Main Menu (incl prompt). Menu will prompt for LCD menu buttons, 5 sec timeout** → `NSS 4.70 BOOT` / `✓+✗ for menu...`
- **Menu buttons ✓+✗ pressed?** — NO (timeout) / YES (✓+✗)
- **Wait for main menu selection** → `--Main Menu--  ↑` / `1.Exit & Boot  ↓`
- **Execute selected menu action**
- **Was "Exit & Boot" selected when ✓ pressed?** — NO / YES → `NSS 4.70 BOOT` / `Start Services`
- **Start Web server** → `NSS 4.70 BOOT` / `Start Network`
- **Setting up Network**
- **Running** → `TSM500-NSS READY` / `IP 192.168.0.201`

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

Main Menu

```
--Main Menu--  ↑      ✓      Start Web server
1.Exit & Boot  ↓
```

```
--Main Menu--  ↑      ✓      Goto TCP/IP Menu
2.TCP/IP...    ↓
```

```
--Main Menu--  ↑      ✓      Goto TLS Menu
3.TLS settings ↓
```

```
--Main Menu--  ↑      ✓      Goto Backup Menu
4.USB Backup...↓
```

```
--Main Menu--  ↑      ✓      Goto Reset Menu
5.Reset...     ↓
```

In all cases, ✖ causes Main Menu to exit and webserver to start

TCP/IP Menu

Goto Main Menu

```
--TCP/IP Menu-  ↑
1.Exit submenu  ↓
```

```
--TCP/IP Menu-  ↑
2.IP Address    ↓
```

```
--TCP/IP Menu-  ↑
3.Netmask       ↓
```

```
--TCP/IP Menu-  ↑
4.Set Gateway   ↓
```

```
--TCP/IP Menu-  ↑
5.Clear Gateway ↓
```

```
IP address*
Confirm Y← →N
```
➤N

```
Edit addr? Y← →N
192.168.000.201
```
➤N

Y◄

```
Address (edit)
101.002.003.004
```
✗

```
186.214.000.204
Save addr? Y← →N
```
➤N

Y◄

Store change

```
Clear Gateway
Confirm Y← →N
```
➤N

Y◄

Store change

In all cases, ✗ returns to the Main Menu

Address* is one of:

IP address, Netmask or gateway

TLS Menu

```
                                                    ┌─────────────────┐
                                              ✓────▶│ Goto Main Menu  │
   ┌──────────────────────┐                         └─────────────────┘
   │ --TLS Menu----   ↑   │
   │ 1.Exit submenu   ↓   │
   └──────────────────────┘

   ┌──────────────────────┐          ┌──────────────────────┐    ┌────┐
   │ --TLS Menu----   ↑   │   ✓────▶ │ Reset keys ?         │    │ ➤N │
   │ 2.Reset keys     ↓   │          │ Confirm Y← →N        │    └────┘
   └──────────────────────┘          └──────────────────────┘
                                               │ Y◄
                                      ┌──────────────────────┐
                                      │ Confirm TLS          │   ✗────▶
                                      │ reset? Y✓ ✗N         │
                                      └──────────────────────┘
                                               │ ✓
                                      ┌─────────────────┐
                                      │   Reset Keys    │─────▶
                                      └─────────────────┘

   ┌──────────────────────┐          ┌──────────────────────┐    ┌────┐
   │ --TLS Menu----   ↑   │   ✓────▶ │ Disable TLS ?        │    │ ➤N │
   │ 3.Disable TLS    ↓   │          │ Confirm Y← →N        │    └────┘
   └──────────────────────┘          └──────────────────────┘
                                               │ Y◄
                                      ┌─────────────────┐
                                      │  TLS Disabled   │─────▶
                                      └─────────────────┘

   ┌──────────────────────┐          ┌──────────────────────┐    ┌────┐
   │ --TLS Menu----   ↑   │   ✓────▶ │ Enable TLS ?         │    │ ➤N │
   │ 4.Enable TLS     ↓   │          │ Confirm Y← →N        │    └────┘
   └──────────────────────┘          └──────────────────────┘
                                               │ Y◄
                                      ┌─────────────────┐
                                      │   TLS Enabled   │─────▶
                                      └─────────────────┘
```

In all cases, ✗ returns to the Main Menu

Backup Menu

```
                                              ┌──────────────────┐
                                         ┌───►│  Goto Main Menu   │◄────────────┐
                                         │    └──────────────────┘             │
  ┌────────────────────────┐   ✓         │                                      │
  │ --Backup Menu-  ↑       ├────────────┘                                      │
  │ 1.Exit submenu  ↓       │◄──────────────────────────────────────────┐      │
  └────────────────────────┘                                            │      │
         │           ▲                                                   │      │
         ∨           ∧                                                   │      │
                              ┌──────────────────────────┐              │      │
  ┌────────────────────────┐  │                          │   ┌────┐      │      │
  │ --Backup Menu-  ↑       │  │ Backup to USB ?          │   │ ➤N │──────┘      │
  │ 2.Backup to USB↓        ├─►│ Confirm Y←  →N           │   └────┘             │
  └────────────────────────┘  └──────────────────────────┘                     │
         │           ▲                    │                                      │
         ∨           ∧              ┌──────────┐                                 │
                                    │  Y◄      │                                 │
                                    └──────────┘                                 │
                                         ∨                                       │
                               ┌──────────────────┐                             │
                               │  Backup to USB   │─────────────────────────────┘
                               └──────────────────┘

  ┌────────────────────────┐   ✓     ┌──────────────────────────┐   ┌────┐
  │ --Backup Menu-  ↑       ├────────►│ USB restore ?            │   │ ➤N │
  │ 3.USB Restore   ↓       │         │ Confirm Y←  →N           │   └────┘
  └────────────────────────┘         └──────────────────────────┘
         └────────┬────────┘                   │
                                         ┌──────────┐
                                         │  Y◄      │
                                         └──────────┘
                                              ∨
                                    ┌──────────────────┐
                                    │ Restore from USB │
                                    └──────────────────┘
```

In all cases, ✘ returns to the Main Menu

Reset Menu

```
Goto Main Menu
```

```
--Reset Menu-    ↑
1.Exit submenu   ↓
```
✓

```
--Reset Menu-    ↑
2.Admin passwd   ↓
```
✓
```
Admin passwd?
Confirm  Y← →N
```
➤N

Y◄
```
Confirm admin
reset? Y✓ ✗N
```
✗

✓
```
Reset TsmWeb Admin user
password (set new password
on next login)
```

```
--Reset Menu-    ↑
3.Config Reset   ↓
```
✓
```
Config reset?
Confirm    Y← →N
```
➤N

Y◄
```
--Reset Menu-    ↑
4.Factory Reset  ↓
```
✓
```
Confirm config
reset? Y✓ ✗N
```
✗

✓
```
Reset config/data to default
values
```

In all cases, ✗ returns to the Main Menu

```
Only for use by
MANUFACTURER
```

```
if Factory Reset confirmed
reset config/data to default
values & automatically reboot
```

```
Start TsmWeb
```
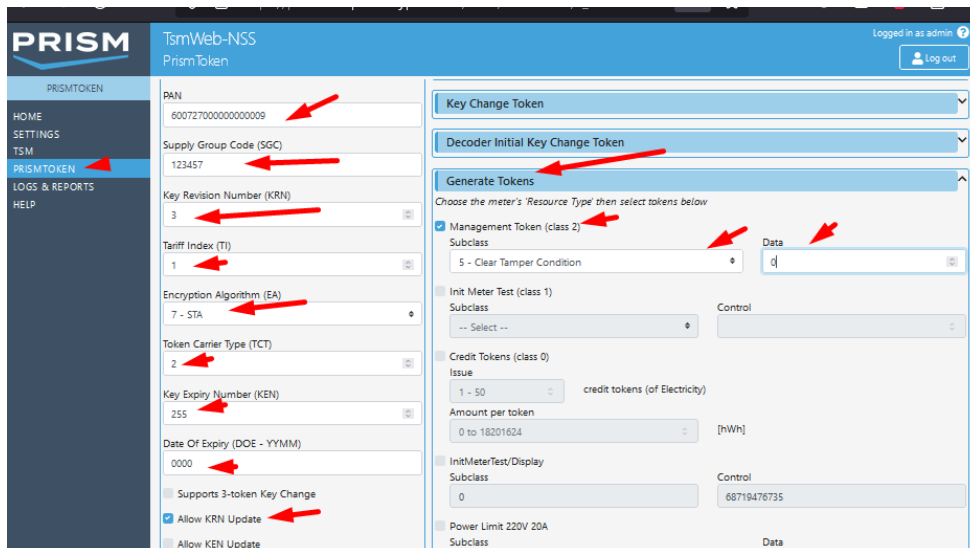
10 Vending Tokens using PrismToken Web UI

PrismToken web UI supports the generation of:-

- Meter Specific Engineering tokens (MSE tokens)
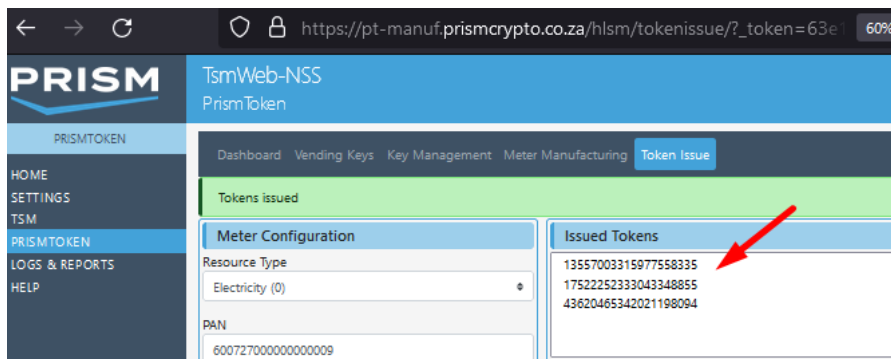
- STS Key Change Tokens

- STS Vend Credit Tokens

10.1 Meter Specific Engineering Tokens

The PrismToken web UI supports the generation of MSE tokens

- Click on "PrismToken" in the left navigation menu, the select the "Token Issue" tab.

- To generate a MSE token for a specific meter: enter the desired meter configuration (ignore the "New Meter Configuration" box), expand the "Generate Tokens" box. By ticking the "Allow KRN Update" box will tell PrismToken that I also want to receive Key Change Tokens to move the meter to the latest available KRN.

- Check the "Management Token (class 2)" box and select subclass and set data. Click on "Generate Tokens"

- The results are as follows: the system has generated three tokens (2 Key Change Tokens, plus one Tamper Token). These tokens will work in meter 600727000000000009 if it has been configured on SGC 123457, KRN 3, TI 1.
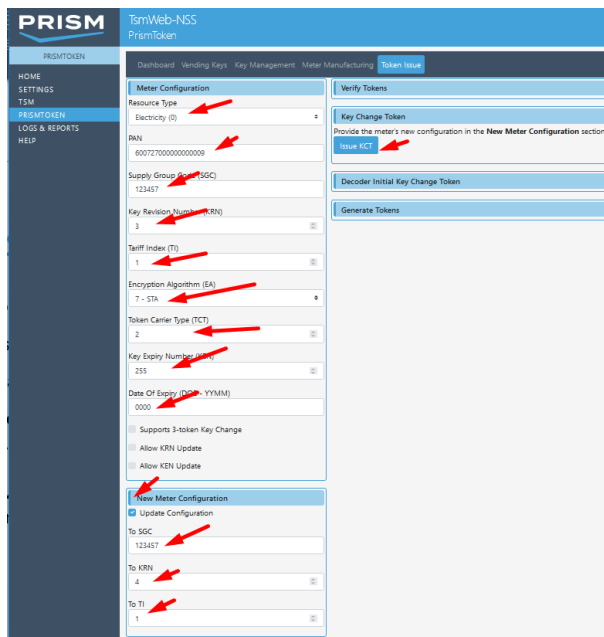
10.2 Vend STS Key Change Token

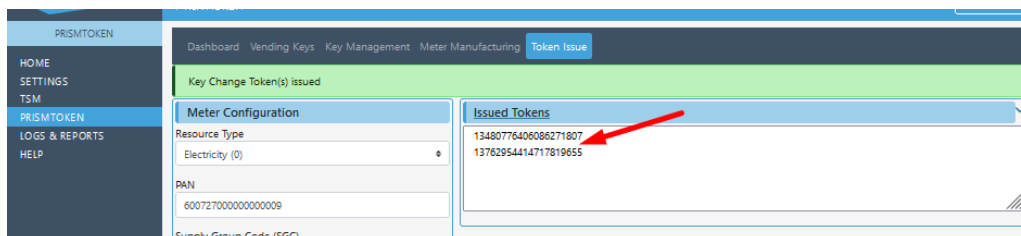The PrismToken web UI supports the generation of STS Key Change Tokens:

- In this example the security module has a 1993 base date key (SGC=123457, KRN=3) and a 2014 base date key (SGC=123457, KRN=4)

- One can generate key change tokens for a meter to change the key revision (KRN) from the 1993 revision number to the 2014 revision number.

- Click on "PrismToken" in the left navigation menu, the select the "Token Issue" tab.

- To generate a KCT token for a specific meter: enter the current meter configuration.
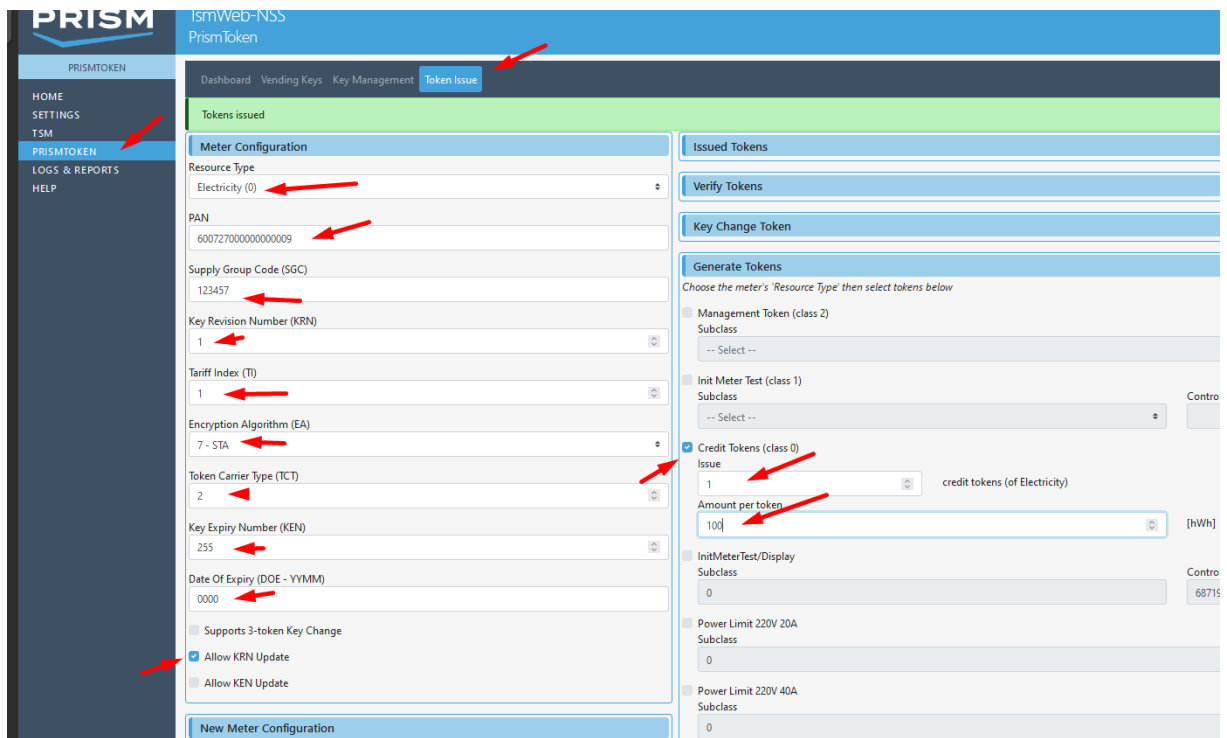
- Check "Update Configuration" and enter the "New Meter Configuration"

- Expand the "Key Change Token" box and click "Issue KCT".

- This key change token will work in meter 600727000000000009 if it has been configured on SGC 123457, KRN 3, TI 1.
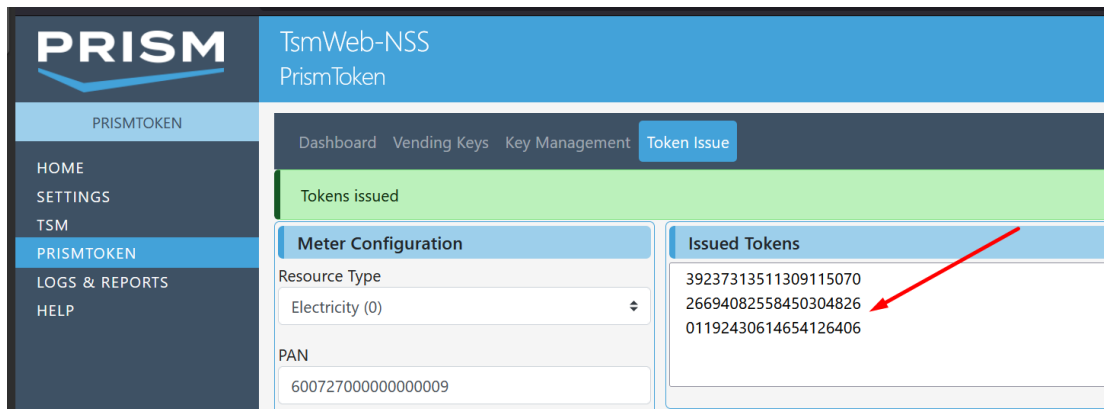

10.3 Vend STS Credit Token

The PrismToken web UI supports the generation of STS Credit Tokens:

- To generate a credit token for a specific meter: enter the "Meter Configuration" information (ignore the "New Meter Configuration" box), expand the "Generate Tokens" box. By ticking the "Allow KRN Update" box will tell PrismToken that I also want to receive Key Change Tokens to move the meter to the latest available KRN.

- Check the "Credit Tokens (class 0)" box and select subclass and set data. Click on "Generate Tokens".

- The example below illustrates generating a single 100 hWh credit token for the electricity meter with PAN 600727000000000009, SGC 123456, KRN 1, TI 1. By ticking the "Allow KRN Update" box will tell PrismToken that I also want to receive Key Change Tokens to move the meter to the latest available KRN. Once the data is entered, I clicked the "Generate Tokens" button at the bottom of the page to generate the tokens.

Prism Payment Technologies (Pty) Ltd | Reg No. 1990/005062/07
Directors: L. Mali, A.M.R. Smith (British) | Company Secretary: C.W. van Straaten

www.prism.co.za

- The results are as follows: the system has generated three tokens (2 Key Change Tokens, plus one Credit Token). These tokens will work in meter 600727000000000009 if it has been configured on SGC 123457, KRN 1, TI 1.

APPENDIX A – List of Abbreviations

BL	Boot Loader
CSP	Critical Security Parameter (for example, a password or a key)
DITK	Decoder Initialisation Transfer Key (also known as "Dispenser ROM Key")
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
I/F	Interface
KCED	Key Component Entry Device
LCD	Liquid Crystal Display
LED	Light Emitting Diode (a coloured lamp)
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSS	Networked Security Server, refer to TSM500i-NSS
PC	Personal Computer, often used to refer to any Windows-based computer
PCI [1]	Payment Card Industry (when referring to security standards)
PCI [2]	Peripheral Component Interconnect (when referring to a computer interface adapter)
PCI HSM	HSM Security Standard set by PCI [1]
PIN	Personal Identification Number
POST	Power-On Self Test
SMK	Storage Master Key
SNMP	Simple Network Monitoring Protocol
STS	Standard Transfer Specification
TPS	Transactions Per Second
TSM500i	The Hardware Security Module (HSM) described in this document
TSM500i-NSS	TSM500i HSM integrated with an embedded computer system in 19" rack-mount case
TsmWeb	Management tool with web interface used for HSMs supplied by Prism
UI	User Interface