STS6 Manufacturing TSM500i NSS User Guide

May 2024

Document number:	PR-D2-1124 Rev 1.2
Release date:	May 2024
Copyright:	© 2024 Prism Payment Technologies (Pty) Ltd
Synopsis:	This document describes the PCI HSM v3.0 STS6 Manufacturing TSM500i-NSS Hardware Security Module (HSM), and the TsmWeb and PrismToken interfaces used to manage this HSM.

Company Confidential

The information in this document is intended only for the person or the entity to which it is addressed and may contain confidential and/or privileged material. Any views, recreation, dissemination or other use of or taking of any action in reliance upon this information by persons or entities other than the intended recipient, is prohibited.

Disclaimer

Prism Payment Technologies (Pty) Ltd makes no representations or warranties whether expressed or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Important Notes

⚠ **This document only applies to a STS6 Manufacturing 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 HSM is shipped with no passwords for the Crypto Officer roles. The two crypto appointed officers must authenticate the HSM on initial deployment and set their passwords in accordance with section 4.3. This step is used to transfer control of the HSM from the Manufacturer to the Customer.**

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

Contents

1 Overview 7
1.1 TSM500i-NSS Description 7
1.2 Key Component Entry Device (KCED) DESCRIPTION 8
2 Setup Quick Guide 9
3 NSS Initial Setup 10
3.1 Inspect and Install Hardware 10
3.1.1 Hardware Inspection 10
3.1.2 TSM500i-NSS Hardware Installation 10
3.2 Check Physical Indicators (LEDs) 11
3.3 Network Setup and Recovery 12
3.3.1 Use the LCD MENU to set the IP address 12
3.4 TsmWeb Interface 13
3.4.1 Invoking TsmWeb for a TSM500i-NSS 13
3.4.2 Setting the TsmWeb admin password 14
3.4.3 Using TsmWeb for the first time 15
3.4.4 Accessing TsmWeb through a different subnet 15
4 HSM Initial Setup 16
4.1 Managing the Secure KCED Service 16
4.2 Pairing the TSM500i HSM with the Secure KCED 17
4.3 Authenticate HSM and Set Initial Passwords 19
4.3.1 Put the TSM500i into the Loader State 19
4.3.2 Authenticate HSM - Request Step 20
4.3.3 Authenticate HSM - Finalise Step 20
4.3.4 Add additional crypto officers 21
5 TsmWeb Initial Setup 22
5.1 Upload PrismToken License Certificate 22
5.2 Setup TsmWeb Users 22
5.2.1 Create users 22
5.2.2 Configuring Account and Password Policy 23
5.2.3 Change Auto-Logoff Timeouts 23
5.2.4 Disable the default admin account 23
5.3 Setup PrismToken Users 23
5.4 Enable PrismToken for Meter Manufacturing 24

5.5 Preferences 24
5.6 Configuring Conductor Service 25
5.6.1 Changing the TCP Port 25
5.6.2 Trace Level Setting 25
5.6.3 Maximum number of socket connections 25
5.6.4 Restarting Conductor 25
5.7 PrismToken Dashboard....25
5.8 Generating and loading the DITK 26
5.8.1 Load DITK.... 26
5.8.2 Generating DITK components 28
5.8.3 DITK Component Sheet Template.... 30
5.8.4 DITK is known 31
5.9 Backup NSS Settings 32
5.10 Upload KMC Public Key 32
5.11 Vending Keys 33
5.11.1 Generate VKLOADREQ 33
5.11.2 Upload KLF into PrismToken.... 34
5.11.3 Load All Vending Keys 35
5.11.4 Load Individual Vending Keys 35
6 Configure and Test Access Service 38
6.1 PrismToken Thrift API....38
6.1.1 Automating PrismToken using the Thrift API 38
6.1.2 Generating STS Tokens by integrating with the thrift API 38
6.2 Conductor....40
7 Security, Operations, and Monitoring 41
7.1 General 41
7.2 Security in a Live Environment 41
7.3 Vending Key Settings at the KMC 41
7.4 PrismToken Setup 42
7.5 Monitoring 42
7.6 Known issues affecting reliability 44
8 Status & Diagnostics 45
8.1 TSM500i Status Information....45
8.2 NSS Log Files 45
8.3 Network Diagnostics....45
8.4 Network Diagnostics (NSS service/firewall specific) 46

8.5 Look at the LCD 46
8.6 TSM500i Status LEDs....46
8.7 Contact Prism Support 46
9 Managing TsmWeb.... 47
9.1 SSL/TLS Certificate....47
9.1.1 SSL / TLS can be disabled (Not Recommended) 47
9.2 Preference Manager 48
10 Managing Your NSS 49
10.1 NSS LCD Menu 49
10.2 Backup and Restore....50
10.2.1 Backup & Restore on a TSM500i-NSS.... 50
10.3 Reset NSS to Default Settings 52
10.3.1 Admin Password Reset 52
10.3.2 Config Reset 52
10.3.3 Factory Reset 52
10.4 Disable TLS from the LCD MENU 52
10.5 Upgrading TSM500i-NSS System Software 53
10.5.1 Software upgrade via USB service port 53
10.5.2 Remote software upgrade via TsmWeb 54
10.6 Configuring SNMP....54
10.7 LCD Menu Sequence....55
11 Managing Your HSM 61
11.1 Pairing with Secure KCED....61
11.2 HSM Password Management 61
11.2.1 How to add a Crypto Officer 61
11.2.2 How to change an Existing Crypto Officer Password or Name 62
11.2.3 Reset One Password 62
11.3 Check Operational vs Privileged state 63
11.4 Upgrading TSM500i firmware 63
11.5 Force a tamper condition 64
12 Vending Tokens using PrismToken Web UI 65
12.1 Manufacturer Key Change Token 65
12.2 Meter Specific Engineering Tokens 66
12.3 Vend STS Key Change Token 67
APPENDIX A – List of Abbreviations 69

1 Overview

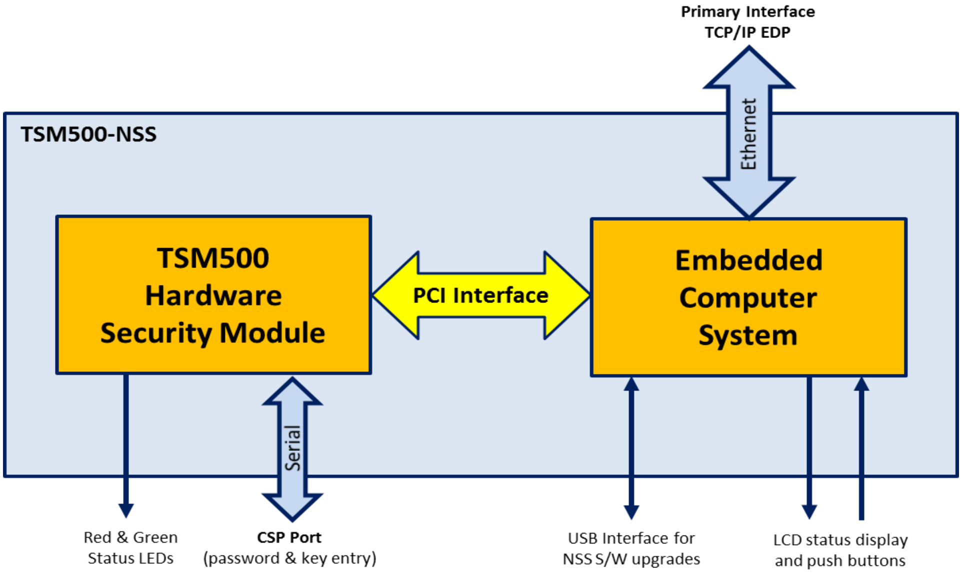
The STS6 Manufacturing TSM500i-NSS is a Hardware Security Module (HSM) and is also referred to as the TSM or HSM in this document. These terms are used interchangeably in the remainder of this document. **This document only applies to the STS6 Manufacturing TSM500i-NSS that has Boot Loader v1.5.0.0 or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

- Load Dispenser ROM Key (DITK) using the KCED
- Generate DITK components and view them on KCED
- 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 Manufacturer Key Change Token

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.


Primary Interface
TCP/IP EDP
Ethernet
TSM500-NSS
TSM500 Hardware Security Module
PCI Interface
Embedded Computer System
Serial
Red & Green Status LEDs
CSP Port (password & key entry)
USB Interface for NSS S/W upgrades
LCD status display and push buttons

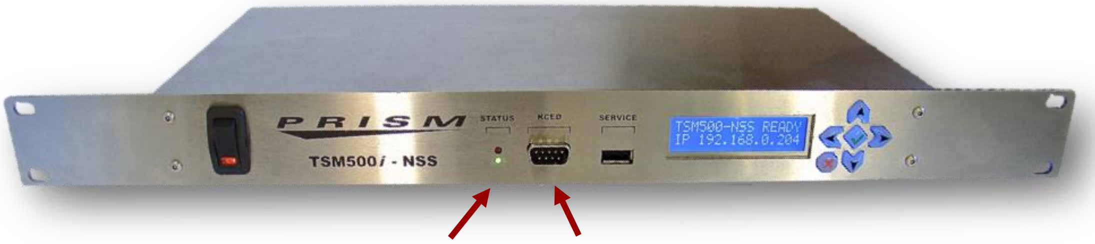
1.2 Key Component Entry Device (KCED) DESCRIPTION

The Key Component Entry Device (KCED) is secure handheld device that is used for the following purposes:

- Entry of Cryptographic Passwords
- Entry of DITK Components
- Generation of DITK Components

Whenever the KCED is connected to the Hardware Security Module (HSM), the Cryptographic Officers must inspect the HSM, the externally connected device, and the inter-connecting cable for any signs of tampering or insertion of a bugging device.

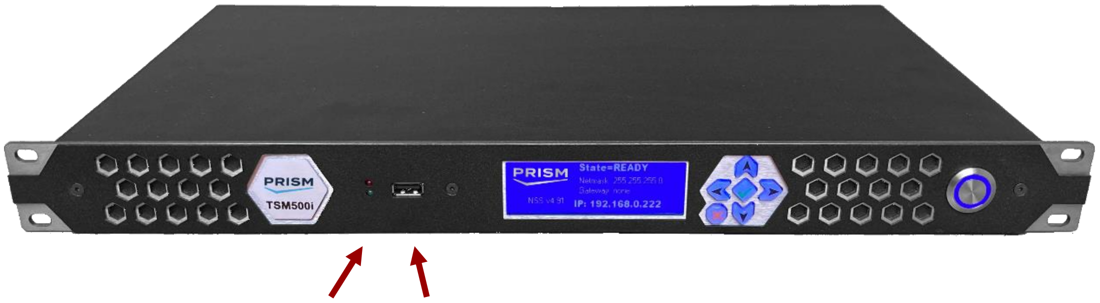
Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently coloured casing, or changes to the serial number or other external markings



TSM500i LEDs **KCED PORT**

Hardware version: 5520-00130_v1.1_NSS

The KCED when used locally connects directly to the TSM500i HSM (Hardware version:5520-00130_v1.1_NSS) using a serial cable to the "KCED" serial port on the front panel.



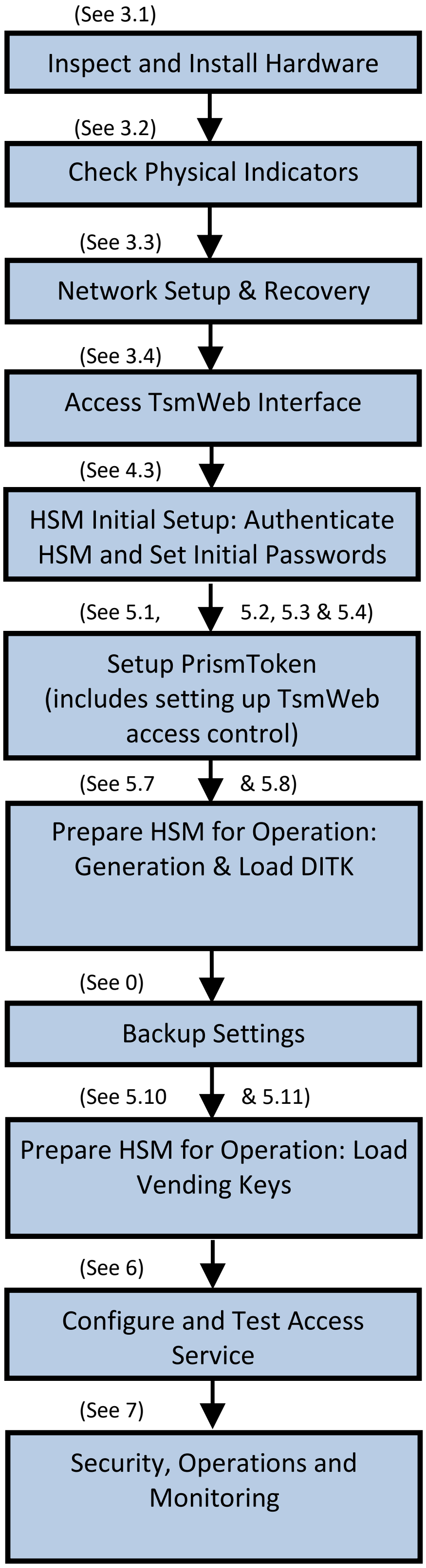
TSM500i LEDs **USB PORT (NSS software updates and KCED)**

Hardware version: 5520-00130_v1.2_NSS

The KCED when used locally connects (Hardware version:5520-00130_v1.2_NSS) using a USB cable to the USB port on the front panel. The KCED USB cable should only be connected when the LCD reports status Ready. The KCED can then be powered on. **Warning:** Connecting/Reconnecting the KCED after powering it on will result the KCED being unable to communicate with the HSM.

For detailed information on how use the KCED, refer to the KCED Installation and User Guide that may be found under the Help menu in TsmWeb.

2 Setup Quick Guide


(See 3.1)
Inspect and Install Hardware
(See 3.2)
Check Physical Indicators
(See 3.3)
Network Setup & Recovery
(See 3.4)
Access TsmWeb Interface
(See 4.3)
HSM Initial Setup: Authenticate HSM and Set Initial Passwords
(See 5.1, 5.2, 5.3 & 5.4)
Setup PrismToken (includes setting up TsmWeb access control)
(See 5.7 & 5.8)
Prepare HSM for Operation: Generation & Load DITK
(See 0)
Backup Settings
(See 5.10 & 5.11)
Prepare HSM for Operation: Load Vending Keys
(See 6)
Configure and Test Access Service
(See 7)
Security, Operations and Monitoring

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

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

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

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.

The TSM500i is shipped ***without Crypto Officer passwords****.*
A two- step process is used to authenticate the HSM at the place of initial deployment, and to simultaneously set the initial 2 crypto officer passwords. This process is used to transfer control of the HSM from the Manufacturer to two Customer crypto officers.

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, setup PrismToken Users, and enable PrismToken to be used in a meter manufacturing environment. If not using PrismToken , then communication with the HSM is via the conductor interface, see 5.6 for more detail.

Access the PrismToken dashboard and navigate to the Meter Manufacturing tab. Once initiated on the web page the DITK components are entered into the HSM using a KCED. After the DITK has been loaded the TSM500i HSM to configure it for operational use. The DITK is split between several custodians in the form of components. EA7 and EA11 DITKs are supported by PrismToken.

Follow the backup procedure to backup TsmWeb settings.

Access the PrismToken dashboard and navigate to the key management tab to upload KMC Public Key into the TSM500i HSM. The meter manufacturer 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.

Client software must be configured to communicate with the PrismToken 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.

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 meter manufacturer tokens can be generated on demand.

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 very important 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)

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.

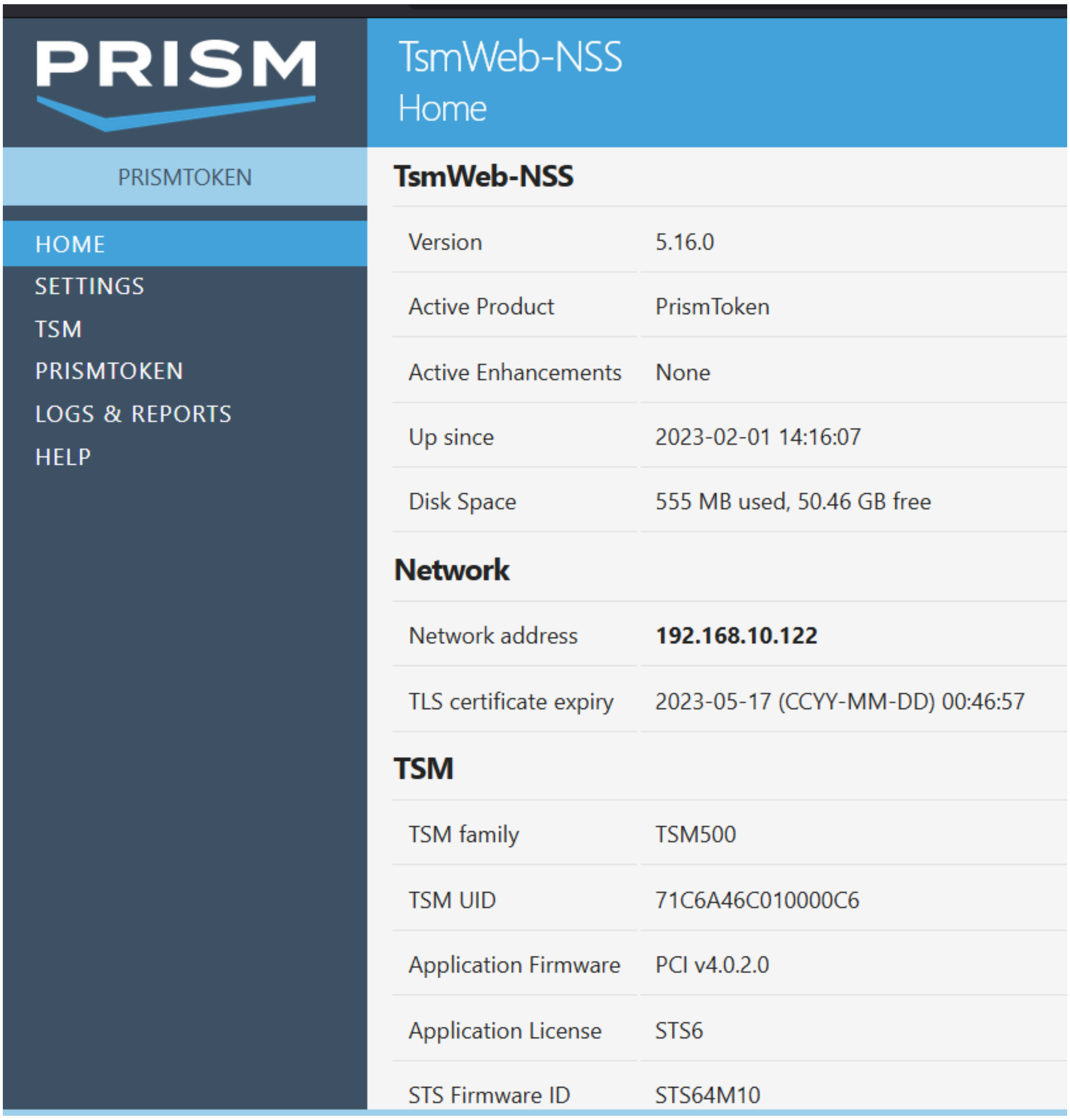
More details about the MAIN MENU can be found in section 10.1.

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).



TsmWeb-NSS

Version	5.16.0
Active Product	PrismToken
Active Enhancements	None
Up since	2023-02-01 14:16:07
Disk Space	555 MB used, 50.46 GB free

Network

Network address	**192.168.10.122**
TLS certificate expiry	2023-05-17 (CCYY-MM-DD) 00:46:57

TSM

TSM family	TSM500
TSM UID	71C6A46C010000C6
Application Firmware	PCI v4.0.2.0
Application License	STS6
STS Firmware ID	STS64M10

3.4.2 Setting the TsmWeb admin password

Please note that TsmWeb is not supplied with default passwords, and it is necessary to set a password 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 **Error! Reference source not found.** 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 HSM Initial Setup

4.1 Managing the Secure KCED Service

⚠ **USB connected Secure KCED: Only connect the Secure KCED to the TSM500i-NSS USB port after the LCD reports status Ready. Then power on the Secure KCED and wait for it to finishing booting.**

Connecting the KCED after powering it on will result it not being able to communicate with the HSM.

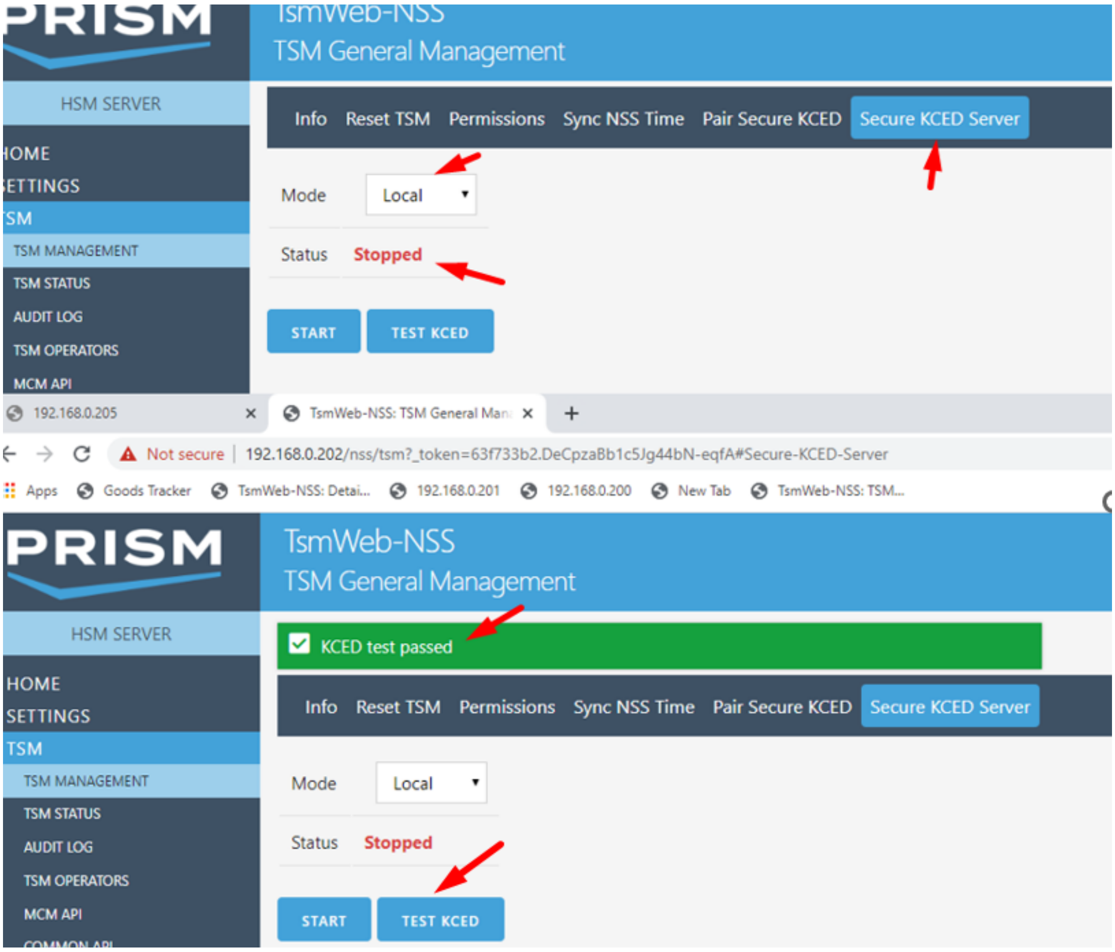
The Secure KCED Service is not applicable to the TSM500i-NSS Hardware version: 5520-00130_v1.1_NSS (stainless steel)

TSM500i-NSS Hardware version: 5520-00130_v1.2_NSS (Black case) this service supports local use of the Secure KCED by default.

Navigate to ***TSM > TSM Management***, and select the "Secure KCED Server" tab.

The service needs to be running in Local mode before you attempting to pair with the Secure KCED connected to the USB port on the front of the TSM500i-NSS. When the service is started the TSM500i-NSS first checks that it can communicate with the Secure KCED.

Click on TEST KCED and confirm that "KCED test pass" is reported. **Note:** If the Secure KCED is not connected to the HSM then the test will fail. If a legacy KCED is connected instead of a Secure KCED the test will also fail. In both cases it will not be possible to start the Secure KCED service.



Mode: Local

Status: Stopped

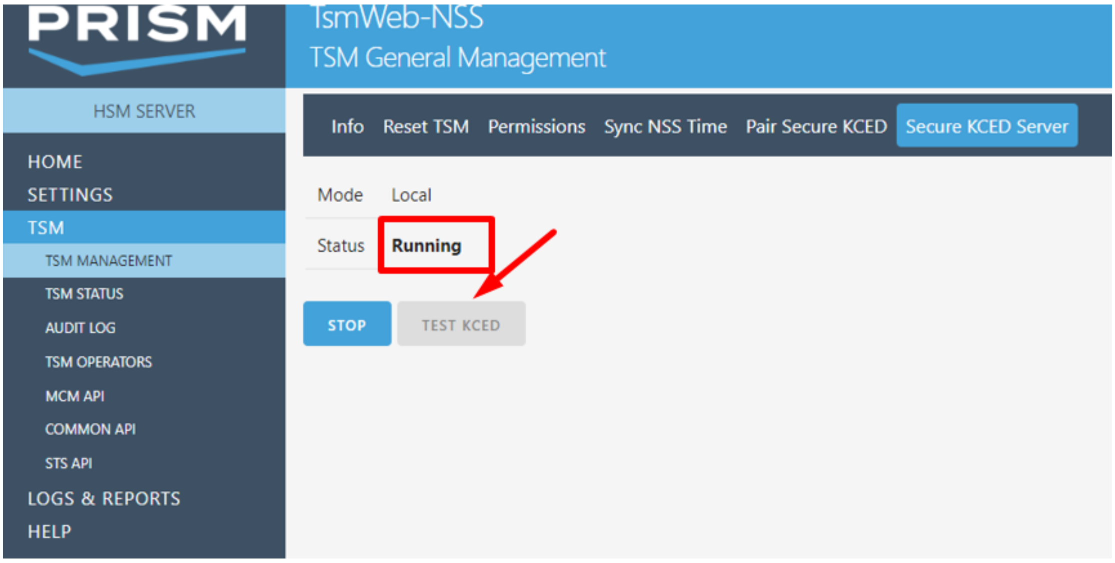
Not secure | 192.168.0.202/nss/tsm?_token=63f733b2.DeCpzaBb1c5Jg44bN-eqfA#Secure-KCED-Server

☑ KCED test passed

Mode: Local

Status: Stopped

Click on “START” and confirm that “Status” changes to “Running”.



Mode Local

Status **Running**

4.2 Pairing the TSM500i HSM with the Secure KCED

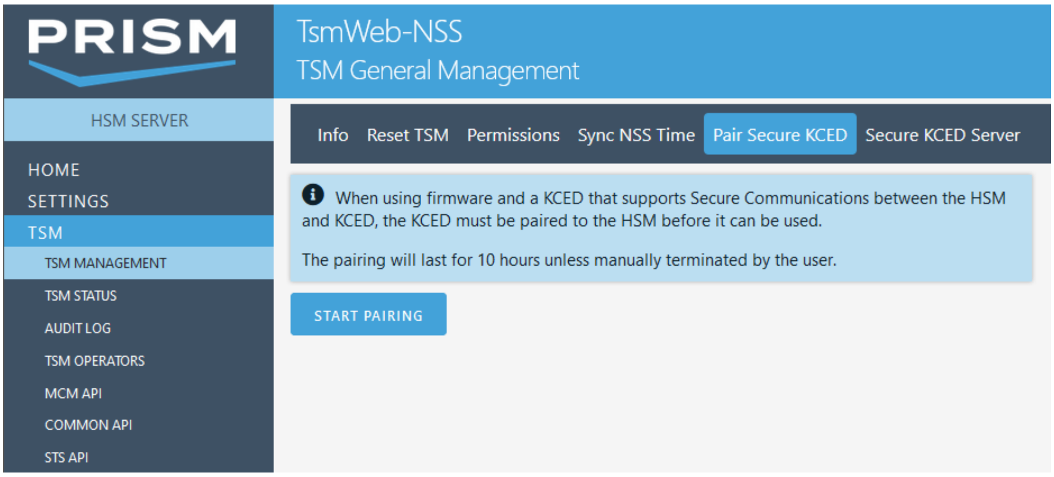
TSM500i HSMs shipped with V1.6.0.0 (or later) Boot loader and V5.0.0.0 (or later) Application firmware must be paired with a Secure KCED, before the Secure KCED can be used to setup Crypto Officers, to display generated components or be used for key component entry.

ⓘ Pairing is not applicable with TSM500i HSMs that have Boot loader earlier than V1.6.0.0 and application firmware earlier than V5.0.0.0.

⚠ **USB connected Secure KCED: Only connect the Secure KCED to the TSM500i-NSS USB port when the LCD reports status Ready. Then power on the Secure KCED and wait for it to finishing booting.**

Connecting the KCED after powering it on will result it not being able to communicate with the HSM.

To pair the KCED with the HSM navigate to ***TSM > TSM Management***, and select the “Pair KCED” tab.

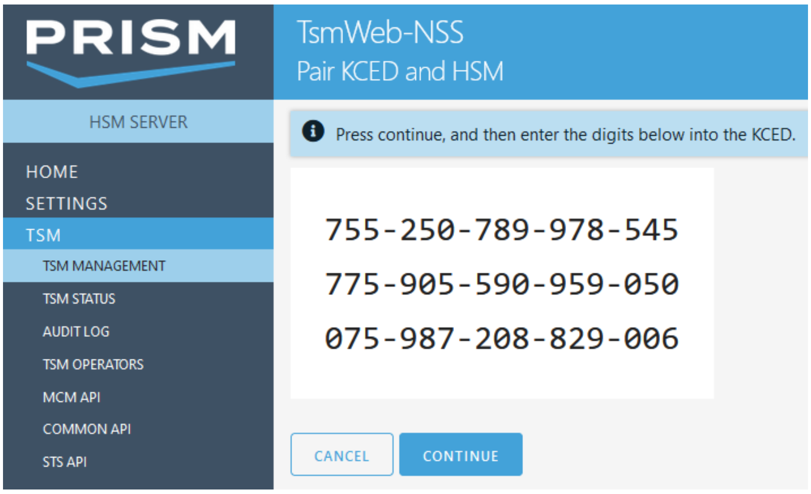


ℹ When using firmware and a KCED that supports Secure Communications between the HSM and KCED, the KCED must be paired to the HSM before it can be used.

The pairing will last for 10 hours unless manually terminated by the user.

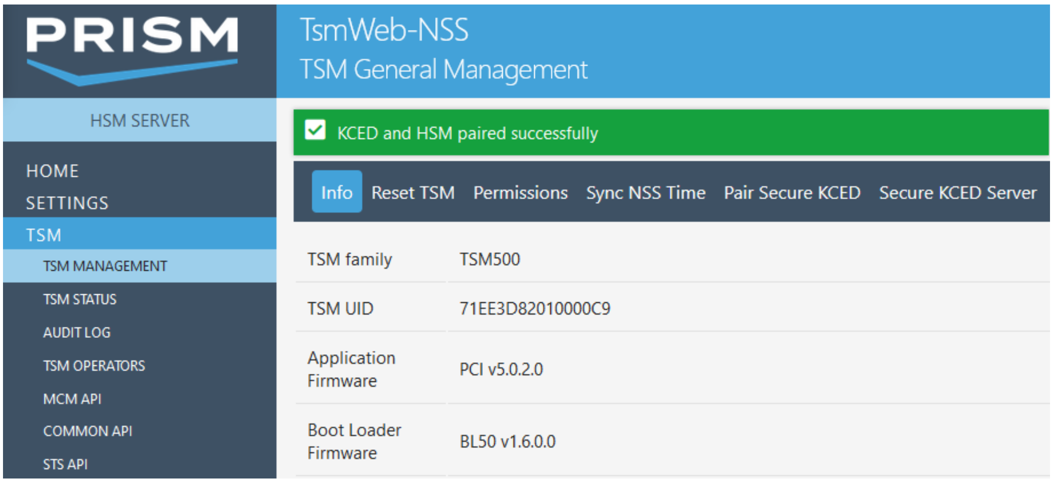
Click on the **Start Pairing** button.

The HSM will generate a 45-digit fingerprint, which will be displayed in TsmWeb. Click on the **Continue** button, after which the 45-digit fingerprint must then be entered on the KCED. You have 180 seconds to enter the fingerprint via the KCED.



Press continue, and then enter the digits below into the KCED.

755-250-789-978-545
775-905-590-959-050
075-987-208-829-006



☑ KCED and HSM paired successfully

TSM family	TSM500
TSM UID	71EE3D82010000C9
Application Firmware	PCI v5.0.2.0
Boot Loader Firmware	BL50 v1.6.0.0

TsmWeb will report the above message if pairing is successful. The pairing state between the TSM500i HSM and the Secure KCED will remain active for 10 hours. The TSM500i HSM can be reset to ***Loader*** state or reset to run the Application multiple times without causing the session with the Secure KCED to be terminated.

If the Secure KCED is power cycled or reboots at any time (during the 10 hours) the secure session will be terminated on the Secure KCED side. Note: that the Secure KCED automatically reboots once a day so that it can run mandatory daily self-tests.

If the session has expired, or has been terminated, then the TSM500i HSM and the KCED will need to be paired again before using the KCED further with the HSM.

4.3 Authenticate HSM and Set Initial Passwords

The two-step process is used to authenticate the HSM at the place of first deployment, and to simultaneously set the initial two (2) Cryptographic Officer passwords. This process is used to transfer control of the HSM from the Manufacturer to two Customer crypto officers.

The TSM500i HSM is shipped without any Cryptographic Officer passwords.

The Cryptographic Officer passwords reside inside the HSM. They must not be confused with, and are not related to, the TsmWeb user account passwords.

This section is not applicable to HSMs running STS6 vending firmware, as device authentication is performed by completing a key refresh with the KMC. No cryptographic officer passwords are required.

Requirements: Logged into TsmWeb and the KCED connected to the TSM500i.

4.3.1 Put the TSM500i into the Loader State

Prior to attempting any of the procedures detailed below, it is necessary to ensure that the TSM500i HSM is in the ***Loader*** state. To do this, click on *TSM* side menu and read the ***Access Control Mode*** that is reported. The *Access Control Mode* specifies:

1. Whether the module is in the ***Loader*** state (i.e. running the Boot Loader), ***Loader Tampered*** state or in the ***Operational*** state (i.e. running the Firmware Application).
2. What *Role* is currently assumed (e.g. none, officer, dual officer)

The following *Access Control Modes* are possible:

BL:LOADER_ROLE_NONE	: *Loader* state, no tamper, not logged in
BL:LOADER_ROLE_OFFICER	: *Loader* state, no tamper, officer logged in
BL:LOADER_ROLE_DUAL_OFFICER	: *Loader* state, no tamper, 2 officers logged in
BL:LOADER_ROLE_USER	: *Loader* state, no tamper, user logged in
BL:TAMPERED_ROLE_NONE	: *Loader Tampered* state, not logged in
BL:TAMPERED_ROLE_OFFICER	: *Loader Tampered* state, officer logged in
BL:TAMPERED_ROLE_DUAL_OFFICER	: *Loader Tampered* state, 2 officers logged in
BL:ERROR	: *Loader Error* state, (login not possible)
AC:OPERATIONAL	: *Application* running
AC:PRIVILEGED	: *Application* running, 2 officers logged in

To change the state from ***Operational*** to ***Loader***, click on “Reset TSM” tab in the ***TSM > TSM Management*** page. Click on Reset To Loader and allow about 20 seconds (until the green LED is flashing) for the TSM500i module to complete its initialisation before attempting to communicate with it again.

4.3.2 Authenticate HSM - Request Step

- On the ***TSM > TSM Operators*** page click on the “Authenticate HSM and Set Initial Passwords” tab.
- Select “Request” from the “Action” drop down menu. Click on the **Request** button.
- Write the “Expected Response” down and keep this safe. It will be of the form “ER12345678”.
- Copy the “Token” into the text file. The token will comprise 112 ascii-hex characters.
- Send the “Token” (Device Authentication Token) to Prism (the Manufacturer) so that the HSM can be authenticated before control is transferred to the Customer.
- In the same email, provide the manufacturer with the names and email addresses of the two crypto officers that will be established during the ‘FINALIZE’ step of this process. This information should be provided on a company letterhead. A Sample Letter for the request is provided in MS Word format document which is available for download from the TsmWeb Help page.

⚠ **Having issued the Request and sent the token to the Manufacturer, DO NOT initiate the Request step again prior to completing the Finalize step detailed below. Authenticating the HSM uses a challenge-response mechanism. The Finalize step will only work if it is the response to the last challenge issued.**

4.3.3 Authenticate HSM - Finalise Step

⚠ **To perform this operation, you must have completed the Request step and received the necessary response from the Manufacturer (Prism). The tokens will be emailed individually to the 2 officers identified in the Request step.**

Both officers need to be present simultaneously to complete this step.

- Confirm that both Crypto Officers have received their Control Transfer Tokens from the Manufacturer.
- Confirm that the Expected Response that was returned by the Manufacturer matches the expected response that was recorded in the first step.
- Select “Finalise” from the “Action” drop down menu.
- Ensure that the KCED is attached to the appropriate port of the HSM and has been paired before proceeding.

⚠ **Whenever the KCED is connected to the HSM, the Cryptographic Officers must inspect the HSM, the externally connected device, and the inter-connecting cable for any signs of tampering or insertion of a bugging device.**

- Officer 1 will be required to enter their name and token. The token will be of the form “0187654321”
- Officer 2 will be required to enter their name and token. The token will be of the form “0287654321”
- Click on the **Finalise** button.
- Officer 1 will be required to enter and confirm their password via the KCED. **Make a record of the password and keep in a safe place**.

  - Officer 2 will be required to enter and confirm their password via the KCED. **Make a record of the password and keep in a safe place**.
  - A password must be at least 7 digits in length, using digits in the range 0 to 9.
- **The crypto officers must keep a record of their passwords in a safe place and ENSURE THAT THEY FULLY UNDERSTAND THE CONSEQUENCES OF LOSING THEIR PASSWORDS!**

⚠ **If all crypto officers forget their passwords, there is NO way to reset the HSM passwords without ERASING ALL CSPs.**

On successful completion of the above step, the HSM will have been authenticated to have originated from the Manufacturer and verified to have not been modified.

4.3.4 Add additional crypto officers

Refer to section 11.2.1 for instructions on how to ADD additional Crypto Officers.

⚠ **The above HSM authentication process included setting up passwords for the two crypto officers that took control of the HSM. If all crypto officers forget their passwords, there is NO way to reset passwords WITHOUT ERASING ALL CSPs.**

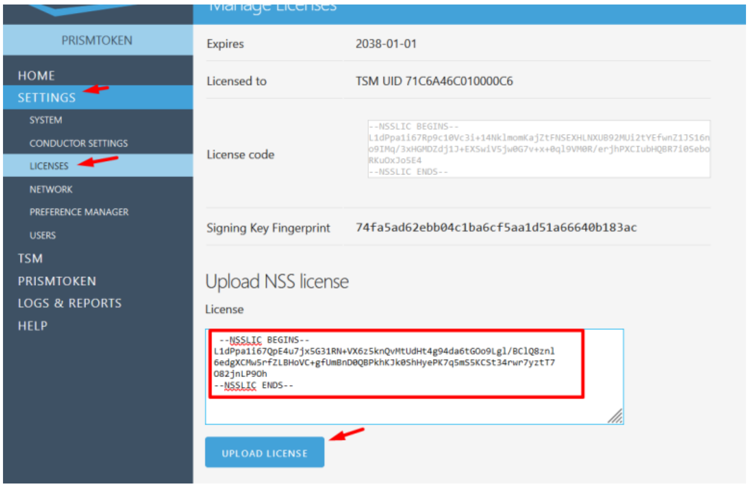
Because the HSM requires dual control for all sensitive operations, it is strongly recommended that the crypto officers add at least one more crypto officer during initial deployment.

5 TsmWeb Initial Setup

5.1 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.



Expires	2038-01-01
Licensed to	TSM UID 71C6A46C010000C6
License code	--NSSLIC BEGINS-- L1dPpa1i67Rp9c10Vc3i+14NklmomKajZtFNSEXHLNXUB92MUi2tYEfwnZ1JS16n o9IMq/3xHGMDZdj1J+EXSwiV5jw0G7v+x+0ql9VM0R/erjhPXCIubHQBR7i0Sebo RKuOxJo5E4 --NSSLIC ENDS--
Signing Key Fingerprint	74fa5ad62ebb04c1ba6cf5aa1d51a66640b183ac

Upload NSS license

License

```
 --NSSLIC BEGINS--
L1dPpa1i67QpE4u7jx5G31RN+VX6z5knQvMtUdHt4g94da6tGOo9Lgl/BClQ8znl
6edgXCMw5rfZLBHoVC+gfUmBnD0QBPkhKJk0ShHyePK7q5mS5KCSt34rwr7yztT7
O82jnLP9Oh
--NSSLIC ENDS--
```

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.**

5.2 Setup TsmWeb Users

5.2.1 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.

5.2.2 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.**

5.2.3 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.

5.2.4 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'.

5.3 Setup PrismToken Users

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

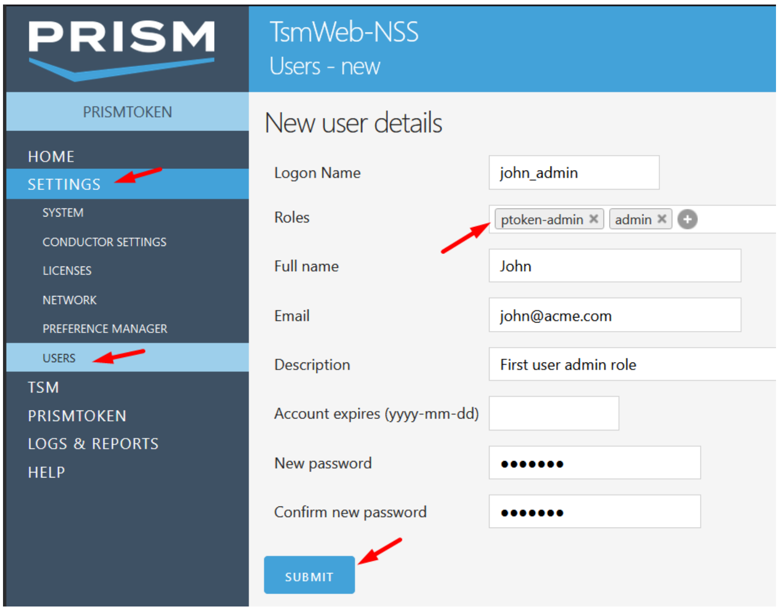
Log into TsmWeb as a user with the 'admin' role (for example, the 'admin' user) and navigate to ***Settings > Users*** page.

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.



New user details

Logon Name	john_admin
Roles	ptoken-admin ✕ admin ✕
Full name	John
Email	john@acme.com
Description	First user admin role
Account expires (yyyy-mm-dd)	
New password	•••••••
Confirm new password	•••••••

5.4 Enable PrismToken for Meter Manufacturing

Log in to TsmWeb as an ‘admin’ ('ptoken-admin role' must be assigned to ‘admin’ account) and set up PrismToken preferences:

Navigate to the ***Settings > Preference Manager*** page.

Find preference “ptoken.meterManufacturingMode”, click “Edit”, and set the value to True. This enables PrismToken to be used in a Meter Manufacturing environment.

Navigate to *Settings > System* page from left navigation menu. Click on “REBOOT NSS” for the preference to take effect. Click on “YES, REBOOT NOW”

5.5 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.

5.6 Configuring Conductor Service

⚠ **Please ignore this section if you are using PrismToken as this section is not 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.

5.6.1 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.

5.6.2 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.

5.6.3 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.

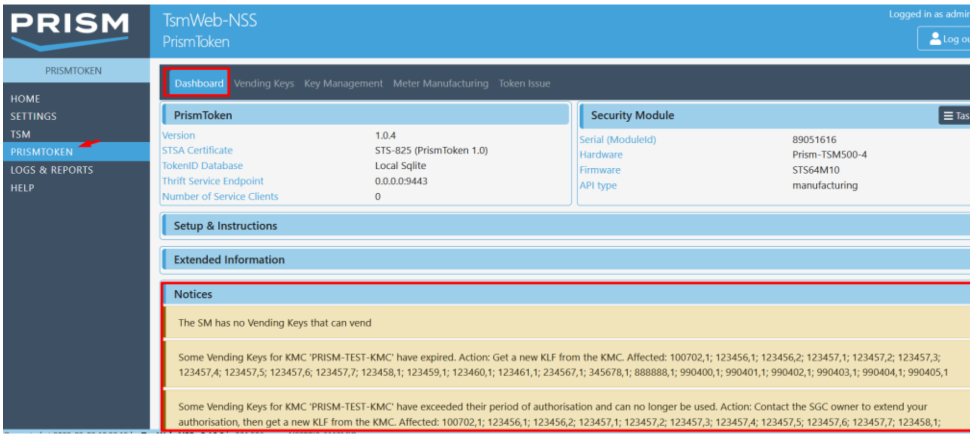
5.6.4 Restarting Conductor

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.

5.7 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.



PrismToken

Version	1.0.4
STSA Certificate	STS-825 (PrismToken 1.0)
TokenID Database	Local Sqlite
Thrift Service Endpoint	0.0.0.0:9443
Number of Service Clients	0

Security Module

Serial (ModuleId)	89051616
Hardware	Prism-TSM500-4
Firmware	STS64M10
API type	manufacturing

Notices

The SM has no Vending Keys that can vend

Some Vending Keys for KMC 'PRISM-TEST-KMC' have expired. Action: Get a new KLF from the KMC. Affected: 100702,1; 123456,1; 123456,2; 123457,1; 123457,2; 123457,3; 123457,4; 123457,5; 123457,6; 123457,7; 123458,1; 123459,1; 123460,1; 123461,1; 234567,1; 345678,1; 888888,1; 990400,1; 990401,1; 990402,1; 990403,1; 990404,1; 990405,1

Some Vending Keys for KMC 'PRISM-TEST-KMC' have exceeded their period of authorisation and can no longer be used. Action: Contact the SGC owner to extend your authorisation, then get a new KLF from the KMC. Affected: 100702,1; 123456,1; 123456,2; 123457,1; 123457,2; 123457,3; 123457,4; 123457,5; 123457,6; 123457,7; 123458,1;

5.8 Generating and loading the DITK

The DITK is also known as the Dispenser ROM key. PrismToken for Meter Manufacturing needs to have at least one DITK loaded to allow newly manufactured meters to be key changed from the DITK. The DITK is entered in the form of components using a Key Component Entry Device (KCED) connected to serial port**. If you choose to use your existing DITK then there is NO need to generate one.**

PrismToken web User Interface (UI) supports full STS6 functionality that includes:

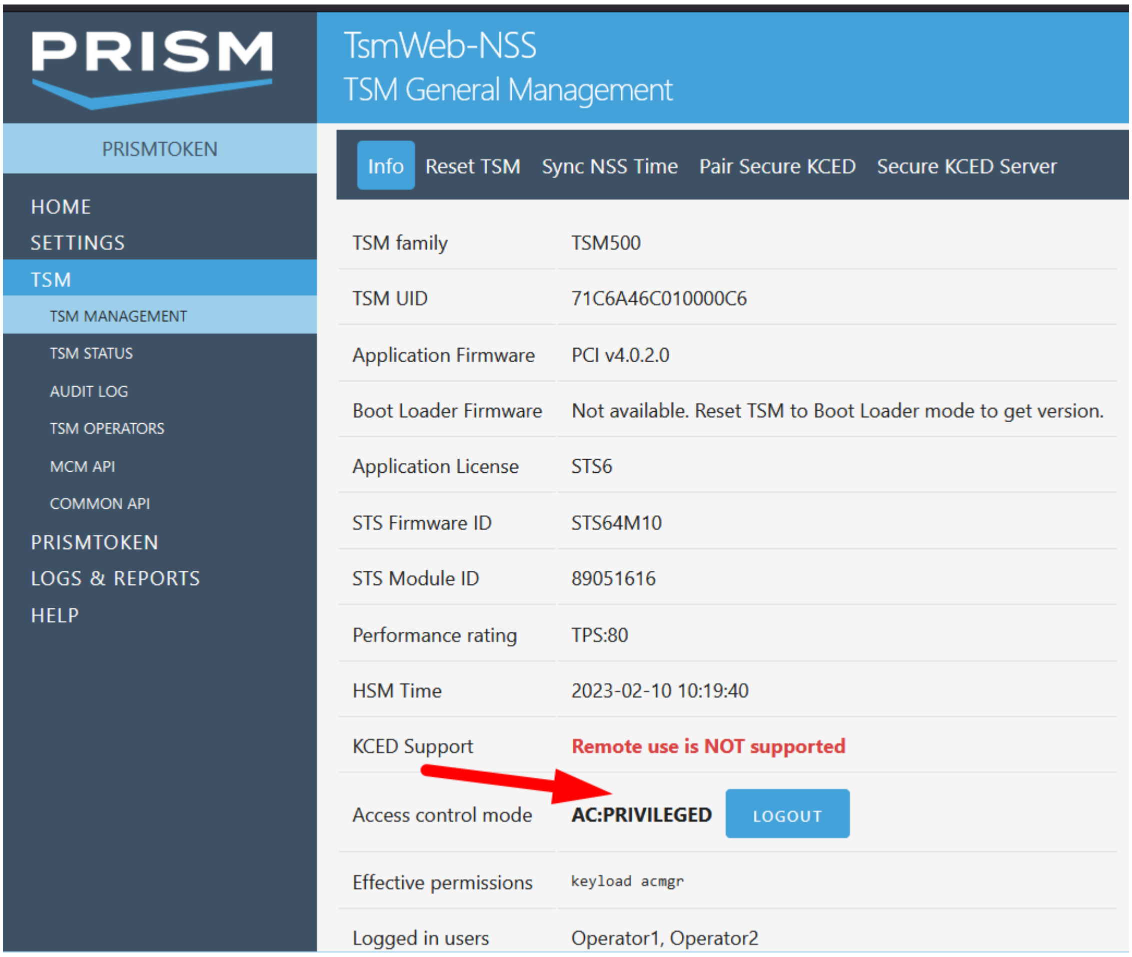
- Generate Dispenser ROM Key (DITK) components for EA7 and EA11 meters and view them on KCED
- Load Dispenser ROM Key (DITK) for EA7 and EA11 meters using the KCED

5.8.1 Load DITK

The DITK must not be confused with, and are not related to, the KLF. The DITK can be generated, and loaded independently of the KLF into the SM.

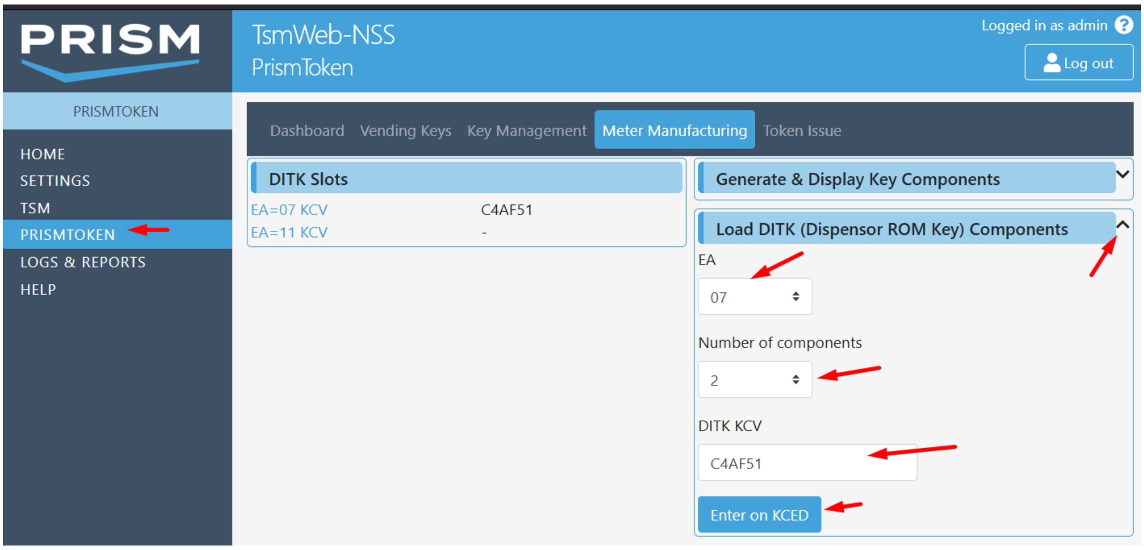
- Connect a KCED to the NSS's "CSP" port which is located on the front of the TSM500i-NSS.
- Set the Security Module into PRIVILEGED state.
    a. Click on the "TSM" tab in the left navigation menu, then select the "TSM Info" tab.
    b. If the page has a warning that the HSM is in Boot Loader mode, then you must reboot the Security Module by selecting the "Reset TSM" tab and clicking "Reset to App".
    c. The "Access control mode" should be "AC:OPERATIONAL", if this isn't the case you should contact support.
    d. On the "TSM Info" tab click on the "Login Operator" button, follow the prompts on the screen and on the KCED. You will be instructed to enter your Crypto Officer passwords.
    e. The "Access control mode" should now be "AC:PRIVILEGED".
    f. The STS6 application firmware will exit the "AC:PRIVILEGED" state automatically if any one of the following conditions are met:
        I. After 30 minutes the HSM will return to operational state.
        II. After 15 minutes where no calls have been made to the HSM.
        III. if more than 50 calls are made then the HSM will return to operational state.

IV. Note that every time you navigate to a different page on TsmWeb this will count towards a call. Some pages require more than one call. Therefore, this may result in the HSM returning to operational state if more than 50 calls are made. It's advised that once you are in Privileged state you should proceed to load DITK immediately.



TSM family	TSM500
TSM UID	71C6A46C010000C6
Application Firmware	PCI v4.0.2.0
Boot Loader Firmware	Not available. Reset TSM to Boot Loader mode to get version.
Application License	STS6
STS Firmware ID	STS64M10
STS Module ID	89051616
Performance rating	TPS:80
HSM Time	2023-02-10 10:19:40
KCED Support	**Remote use is NOT supported**
Access control mode	**AC:PRIVILEGED**
Effective permissions	`keyload acmgr`
Logged in users	Operator1, Operator2

- Click on the "PrismToken" left in the left navigation menu, select the "Meter Manufacturing" tab. Click "Load DITK (Dispenser ROM Key) Components" to expand the box. Select the EA, the number of components that were generated for the key, and have one of the custodians enter the key's KCV, then click "Enter on KCED". Each key custodian must follow the instructions on the KCED, which will prompt them to enter their key component.



DITK Slots

EA=07 KCV	C4AF51
EA=11 KCV	-

EA: 07

Number of components: 2

DITK KCV: C4AF51

- Once the DITK is loaded the KCV will be shown in the "DITK Slots" box. If a dash ("-") is shown, then no DITK has been loaded for that EA.

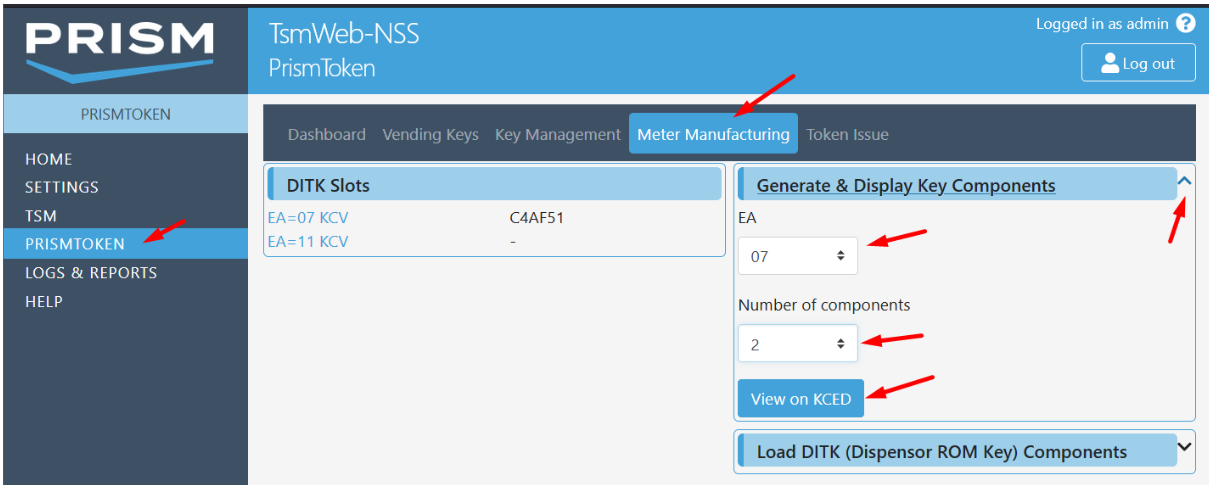
5.8.2 Generating DITK components

Proper measures must be taken to ensure that each component generated is visible to nobody except the custodian responsible for the component otherwise the DITK could be compromised.

There are separate DITKs for EA=07 which is the STS algorithm and EA=11 which is the MISTY1 algorithm. If you do not manufacture EA=11 meters, then you will only require an EA=07 DITK. Each DITK requires two or three components and a Key Check Value (KCV). You can generate the DITK using PrismToken or use a pre-existing DITK. If you choose to use a pre-existing DITK that was not generated using PrismToken please refer to section 5.8.4. The DITK must be generated and stored in the form of components, which are split between two or three trusted custodians. The key components are generated such that combining all components using XOR will yield the DITK.

To generate a DITK:

- Ensure that the module is in the "AC:PRIVILEGED" state as mentioned at the beginning of this section.
- Click on the "PrismToken" left in the left navigation menu.
- Select the "Meter Manufacturing" tab. Click "Generate & Display Key Components" to expand the box.



DITK Slots

EA=07 KCV	C4AF51
EA=11 KCV	-

EA: 07

Number of components: 2

- Select the EA and the number of components (equal to the number of custodians who will look after the key), then click “View on KCED”.
- It is important to note that generating an EA7 DITK using the PrismToken UI will generate an ODD parity DITK.
- This is consistent with our recommendation that the EA7 DITK is generated with ODD parity, as the check digits (KCV) ignore the parity bits.
- Each key custodian must follow the instructions on the KCED, write down their component, component KCV, and DITK KCV, and keep the written component stored in a safe place. For convenience a DITK component sheet template is provided in section 5.8.3 below.
- You will need these components whenever you need to load the DITK into the Security Module (typically immediately and in case of disaster recovery).
- You will need to repeat this process if you want to generate another DITK.

5.8.3 DITK Component Sheet Template

Key name ______________________________

IDENTIFYING NAME OR DESCRIPTION OF THE KEY

Date ______________________________

YYYY/MM/DD OF KEY / COMPONENT CREATION

Generated by ______________________________

FULL NAME AND CONTACT NUMBER OF CUSTODIAN (AT KEY GENERATION)

Component number ______ *of* _______ Algorithm (circle one right): EA7 / EA11

Component *Fill in those parts that are applicable.*

Part 1: *(For EA7 and EA11 DITK components)*

□□□□ □□□□ □□□□ □□□□

Part 2: *(Only for EA11 DITK key components)*

□□□□ □□□□ □□□□ □□□□

Component Check value

□□□□□□

Key Check Value

□□□□□□

5.8.4 DITK is known

It is important to note:

- The meter manufacturer must check whether the process of injecting the key into the meter, or possibly the meter itself, modifies the DITK in any way before using it (e.g. by setting parity to ODD), and ensure that the DITK loaded into the SM must match the actual DITK used by the meter.
- We would recommend using the STS Simulator (available from the STS Association) to generate a "Clear Tamper" token under the DITK that you think is being used by the meter. If the token is accepted by the meter then the DITK is correct.
- Some meter manufacturers who used STS/Legacy firmware loaded their DITK using the SM?IK with (S)et Parity option. They in particular must take care to understand what actual DITK value is used by the meter.
- The DITK loaded into the HSM must match the actual DITK used by the meter.

If your DITK is already known, you must assign components such that if you combine all the components using XOR it will yield the DITK. The DITK could be split between two or three custodians. If you choose to split your DITK between two custodians then you will require two components, alternatively if you choose to split your DITK between three custodians you will require three components.

For example if your actual EA7 DITK used by the meter is x'7676767676767676 (KCV = x'4CBE91) you could choose to split it between two or three components therefore having two or three custodians.

Below is an example of the DITK being split amongst 2 components.

DITK Component 1	x'0000000076767676
DITK Component 2	x'7676767600000000
DITK Component 1 XORED DITK Component 2	x'7676767676767676 (DITK)

⚠ **It is important to note that with reference to the EA7 DITK, the KCV calculation ignores the parity bits, and that if the meter and the HSM are using keys that differ only in parity bits the KCV will be the same, but the crypto operations will fail !!**

5.9 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 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.

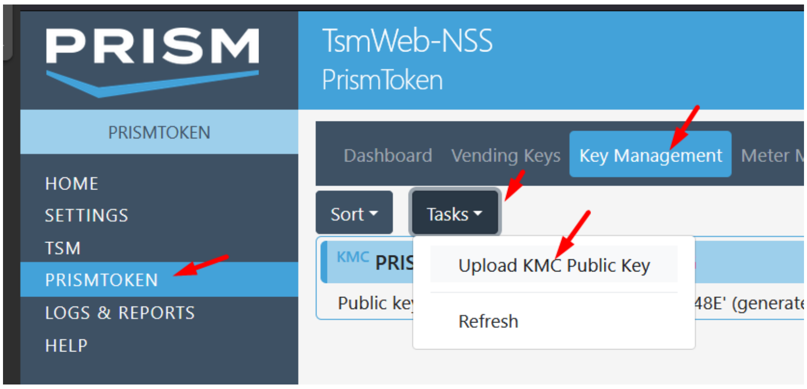
Drives formatted with FAT32 have a 4Gb file size limit which may cause the backup to fail if the database is large.

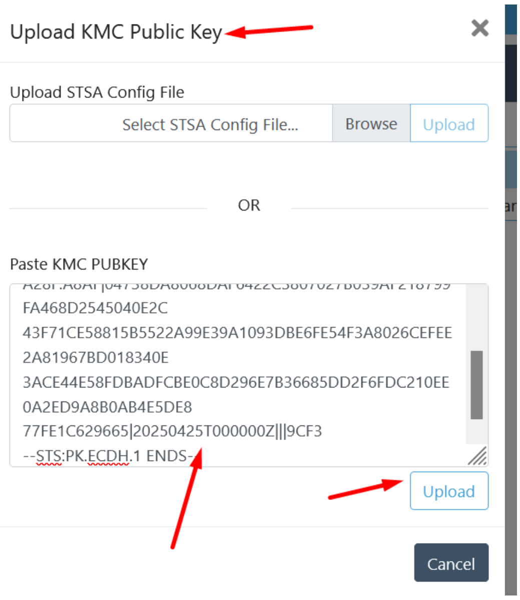
If the backup fails due to lack of disk space or file-size limit then the “boot_log.txt” or “tsmweb_startup_log.txt” will contain a message like “backup failed: database or disk is full”.

5.10 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".





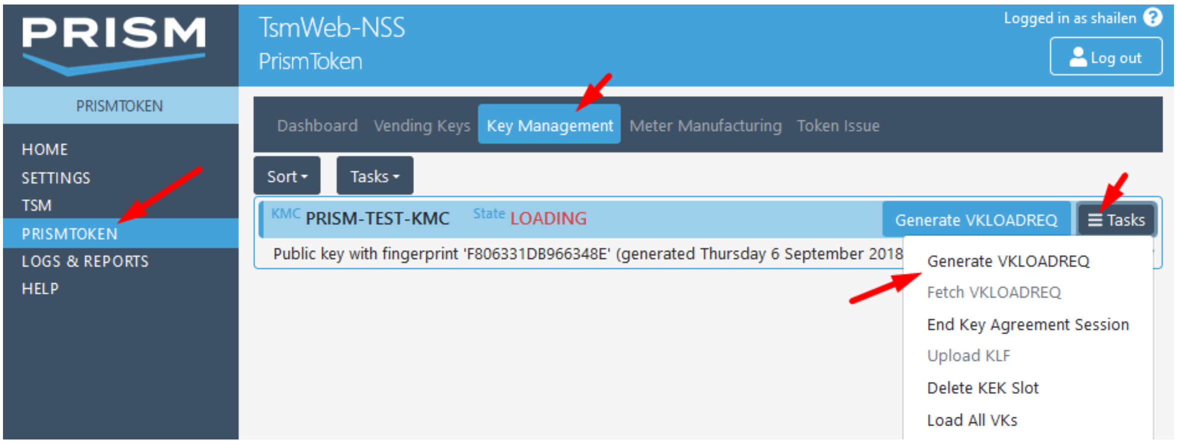
```
FA468D2545040E2C
43F71CE58815B5522A99E39A1093DBE6FE54F3A8026CEFEE
2A81967BD018340E
3ACE44E58FDBADFCBE0C8D296E7B36685DD2F6FDC210EE
0A2ED9A8B0AB4E5DE8
77FE1C629665|20250425T000000Z|||9CF3
--STS:PK.ECDH.1 ENDS--
```

- 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".

5.11 Vending Keys

5.11.1 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.

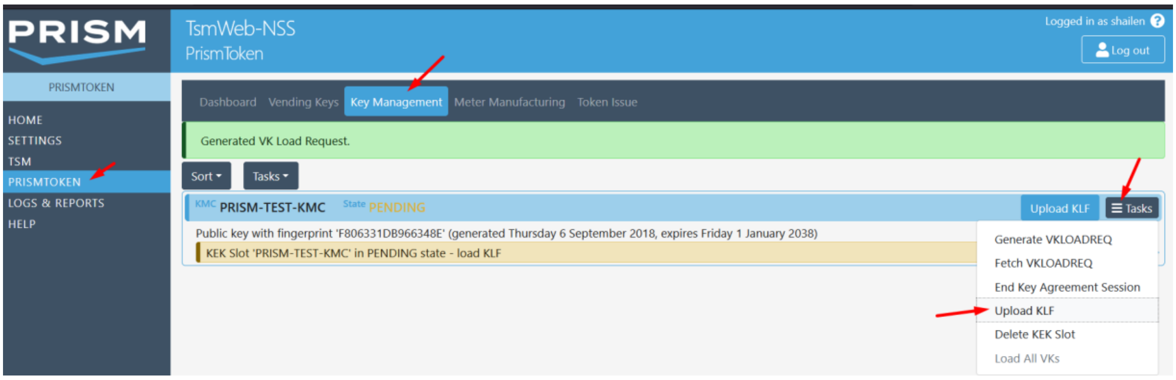


Public key with fingerprint 'F806331DB966348E' (generated Thursday 6 September 2018

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.

5.11.2 Upload KLF into PrismToken

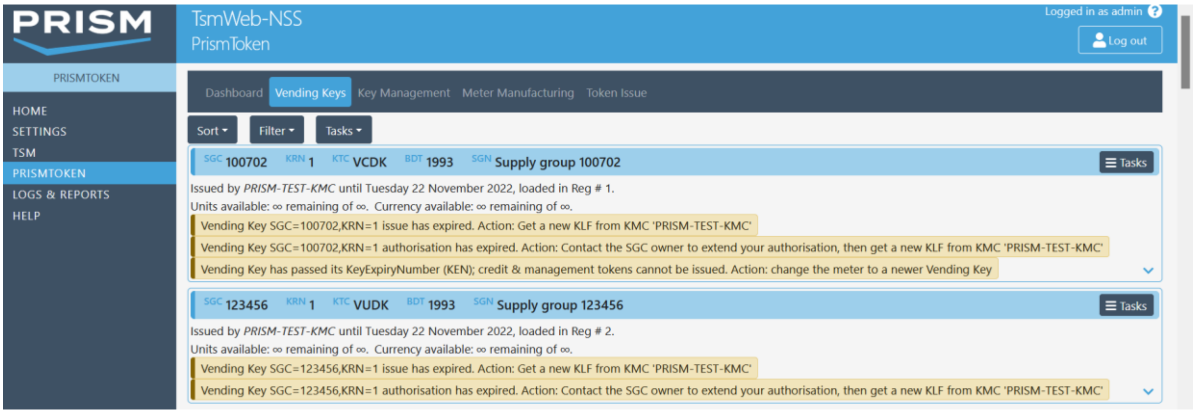
The KMC will reply with an e-mail that has a Key Load File attached. To upload the Key Load File, go to PrismToken, click on “Key Management” tab, the KMC’s “Tasks” menu, and choose “Upload KLF”. You can then navigate to PrismToken’s “Vending Keys” tab where you will see your vending keys. **At this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



Generated VK Load Request.

Public key with fingerprint 'F806331DB966348E' (generated Thursday 6 September 2018, expires Friday 1 January 2038)

KEK Slot 'PRISM-TEST-KMC' in PENDING state - load KLF



SGC 100702 KRN 1 KTC VCDK BDT 1993 SGN Supply group 100702

Issued by *PRISM-TEST-KMC* until Tuesday 22 November 2022, loaded in Reg # 1.
Units available: ∞ remaining of ∞. Currency available: ∞ remaining of ∞.

Vending Key SGC=100702,KRN=1 issue has expired. Action: Get a new KLF from KMC 'PRISM-TEST-KMC'

Vending Key SGC=100702,KRN=1 authorisation has expired. Action: Contact the SGC owner to extend your authorisation, then get a new KLF from KMC 'PRISM-TEST-KMC'

Vending Key has passed its KeyExpiryNumber (KEN); credit & management tokens cannot be issued. Action: change the meter to a newer Vending Key

SGC 123456 KRN 1 KTC VUDK BDT 1993 SGN Supply group 123456

Issued by *PRISM-TEST-KMC* until Tuesday 22 November 2022, loaded in Reg # 2.
Units available: ∞ remaining of ∞. Currency available: ∞ remaining of ∞.

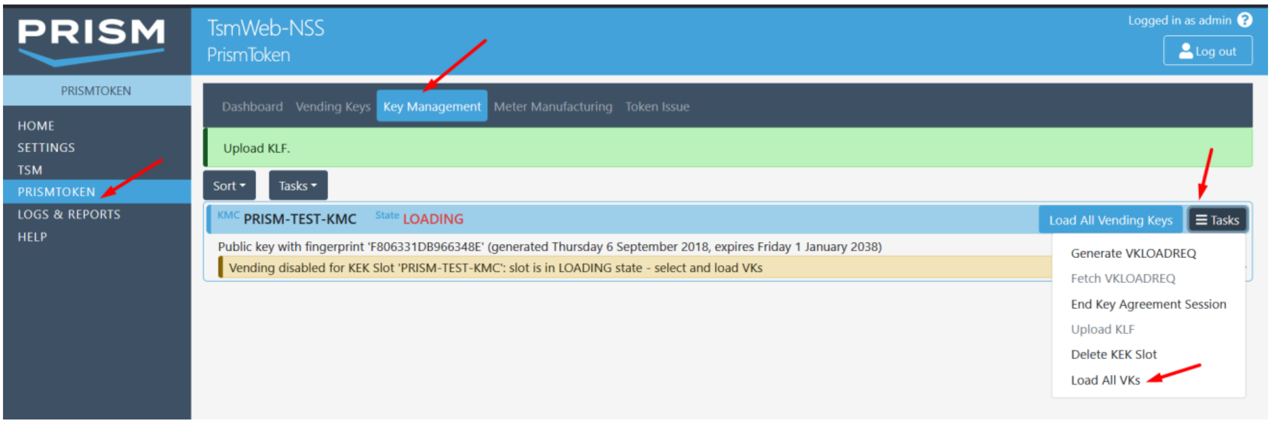
Vending Key SGC=123456,KRN=1 issue has expired. Action: Get a new KLF from KMC 'PRISM-TEST-KMC'

Vending Key SGC=123456,KRN=1 authorisation has expired. Action: Contact the SGC owner to extend your authorisation, then get a new KLF from KMC 'PRISM-TEST-KMC'

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 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.

5.11.3 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.



Upload KLF.

PRISM-TEST-KMC LOADING

Public key with fingerprint 'F806331DB966348E' (generated Thursday 6 September 2018, expires Friday 1 January 2038)

Vending disabled for KEK Slot 'PRISM-TEST-KMC': slot is in LOADING state - select and load VKs

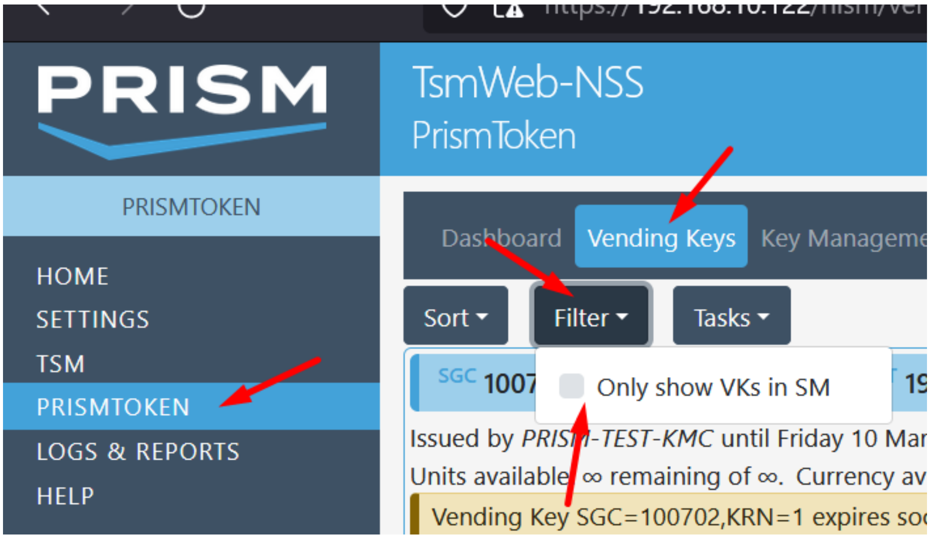
To load the keys from the KLF you will need to select the “Load All VKs” option from the “Tasks” menu. Take note that if the key agreement session is ended before loading all the vending keys, then it will not be possible to load vending keys from the same KLF file into the security module. A new VKLOADREQ 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 5.11.4 if “Load All VKs” returns the following error Failed to load all VKs: STS API error VK_REG_NOT_FOUND_ERROR (code 28)

5.11.4 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.

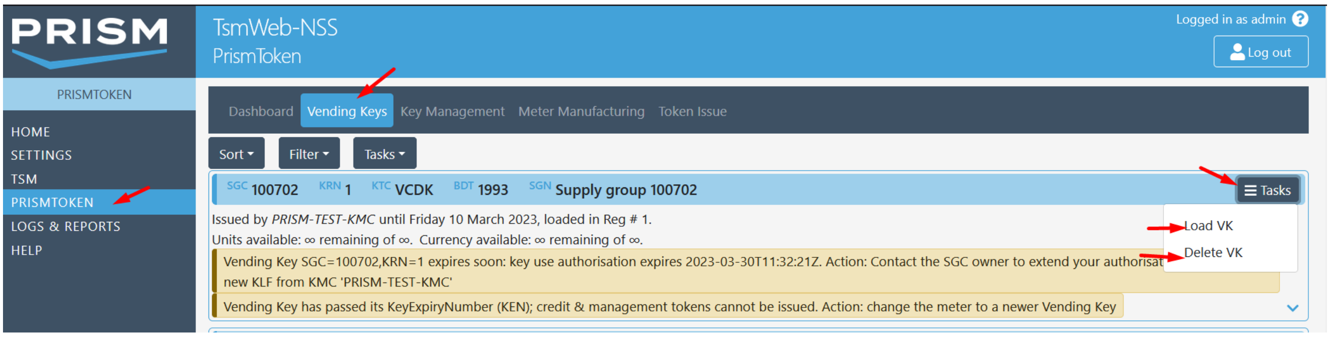


Issued by *PRISM-TEST-KMC* until Friday 10 Mar

Units available: ∞ remaining of ∞. Currency av

Vending Key SGC=100702,KRN=1 expires soo

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.



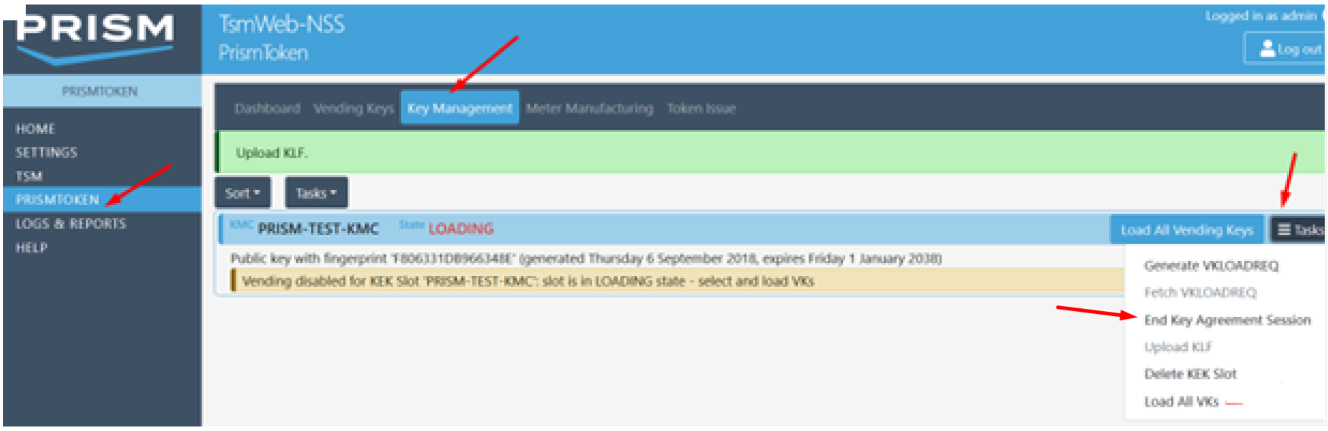
Issued by *PRISM-TEST-KMC* until Friday 10 March 2023, loaded in Reg # 1.

Units available: ∞ remaining of ∞. Currency available: ∞ remaining of ∞.

Vending Key SGC=100702,KRN=1 expires soon: key use authorisation expires 2023-03-30T11:32:21Z. Action: Contact the SGC owner to extend your authorisat new KLF from KMC 'PRISM-TEST-KMC'

Vending Key has passed its KeyExpiryNumber (KEN); credit & management tokens cannot be issued. Action: change the meter to a newer Vending Key

The key agreement session <u>can</u> be ended after loading the individual vending keys to complete the process HOWEVER in the case of manufacturing firmware it is not necessary to close the key management session: the STS Manufacturing Commands can be used while the session is open (KEK Slot is in “Loading” state). The reason for this is some manufacturers may have more vending keys in the KLF than there are slots in the SM. The meter manufacturer can choose which keys they wish to have in the SM and then they can replace one or more without having to get a new KLF.



Upload KLF.

Public key with fingerprint 'F806331DB966348E' (generated Thursday 6 September 2018, expires Friday 1 January 2038)

Vending disabled for KEK Slot 'PRISM-TEST-KMC': slot is in LOADING state - select and load VKs

6 Configure and Test Access Service

6.1 PrismToken Thrift API

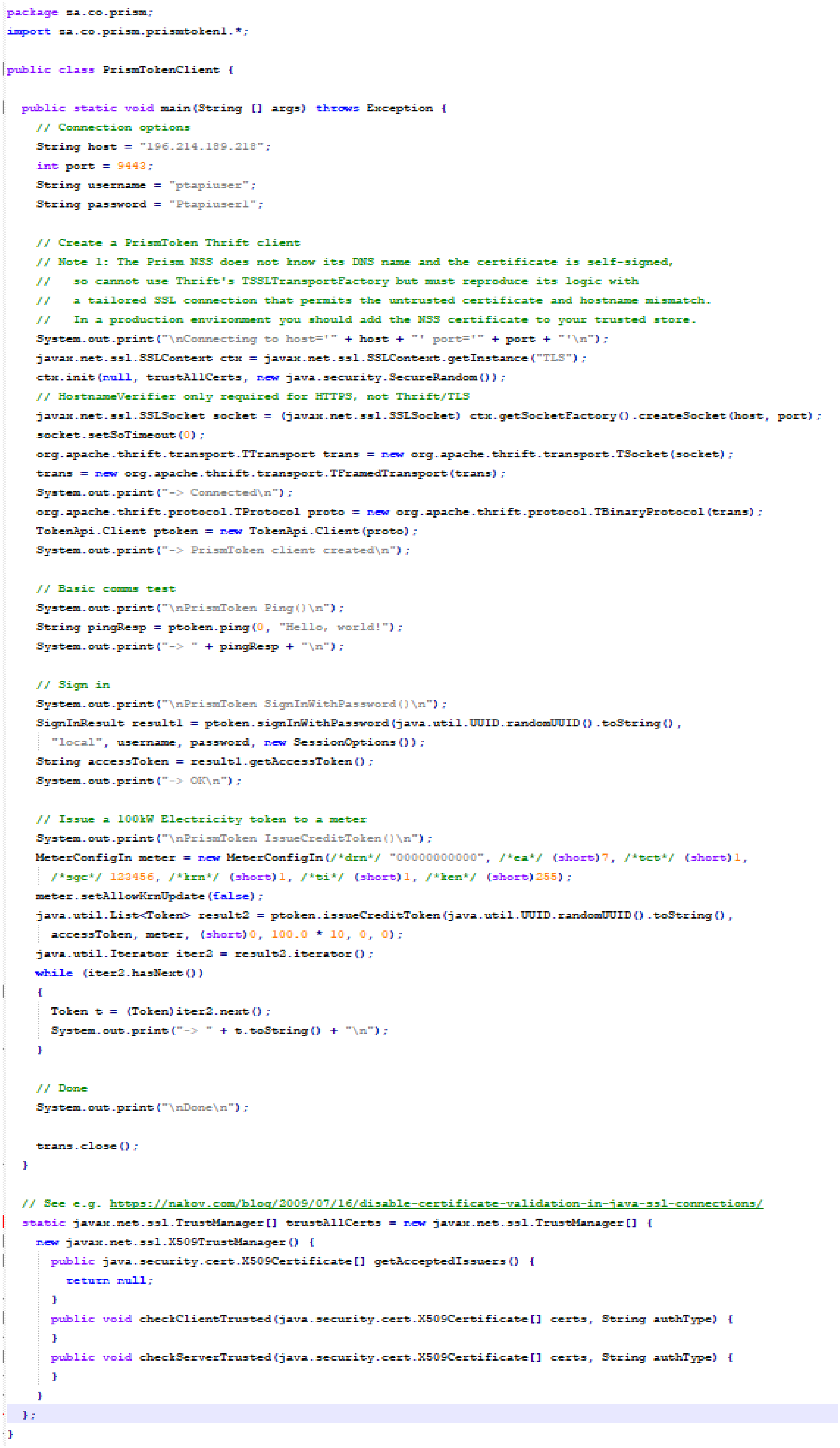
6.1.1 Automating PrismToken using the Thrift API

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).

6.1.2 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 sa.co.prism;
import sa.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) {
      }
    }
  };
}
```

6.2 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.

7 Security, Operations, and Monitoring

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

7.1 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.

7.2 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.
    - 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.
    - 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.

7.3 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.

7.4 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).

7.5 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.
    - After generating a new certificate, you will need to add the new certificate to the trusted stores of your clients, as explained in 7.2 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:

  - 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.
  - 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.
  - 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.
  - 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.
  - 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.
  - 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:
  - 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:
  - 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.

7.6 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.

8 Status & Diagnostics

8.1 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.

8.2 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.

8.3 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

8.4 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.

8.5 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.

8.6 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.

8.7 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.

9 Managing TsmWeb

9.1 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.

9.1.1 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.

9.1.1.1 *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.

9.2 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 5.9) all the preferences are included in the backup.

10 Managing Your NSS

10.1 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 10.3.1
• Set IP Address, Netmask, default gateway	- refer to section 3.3.1
• USB Backup & Restore	- refer to section 5.9
• Reset to Defaults	- refer to section 10.3
• Disable SSL/TLS, reset TLS key	- refer to section 10.4

10.2 Backup and Restore

10.2.1 Backup & Restore on a TSM500i-NSS

Backup

Refer to section 5.9 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 (**Error! Reference source not found.**) 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.

10.3 Reset NSS to Default Settings

Section 10.1 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:

10.3.1 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.

10.3.2 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")

10.3.3 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".

10.4 Disable TLS from the LCD MENU

Using the LCD MAIN MENU as described in section 10.1, select the "Disable TLS" option and confirm the operation. The TLS service is now disabled.

10.5 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.

10.5.1 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

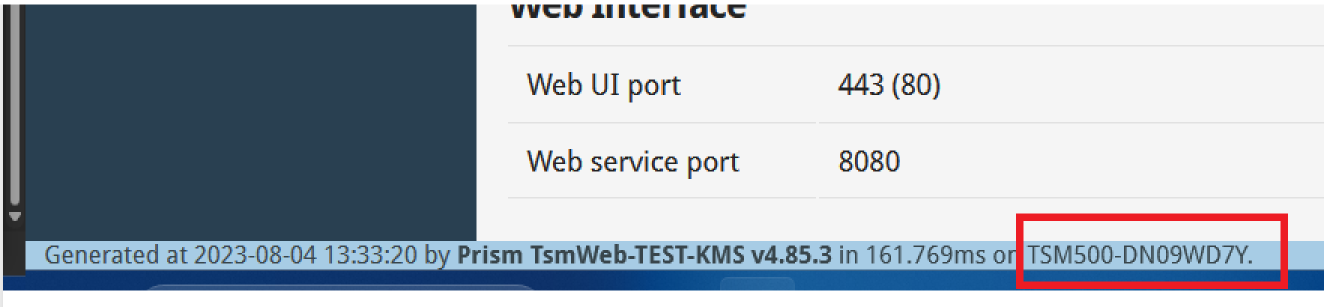
NSS v4.75 introduces a new database structure that improves disk space utilization. The process of upgrading to v4.75 (or higher) includes a mandatory and automatic backup, plus a database migration (that is performed via an automatic restore). The USB flash drive that contains the NSS_UPDATES directory 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.

10.5.2 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 on TSM500-DN09WD7Y.

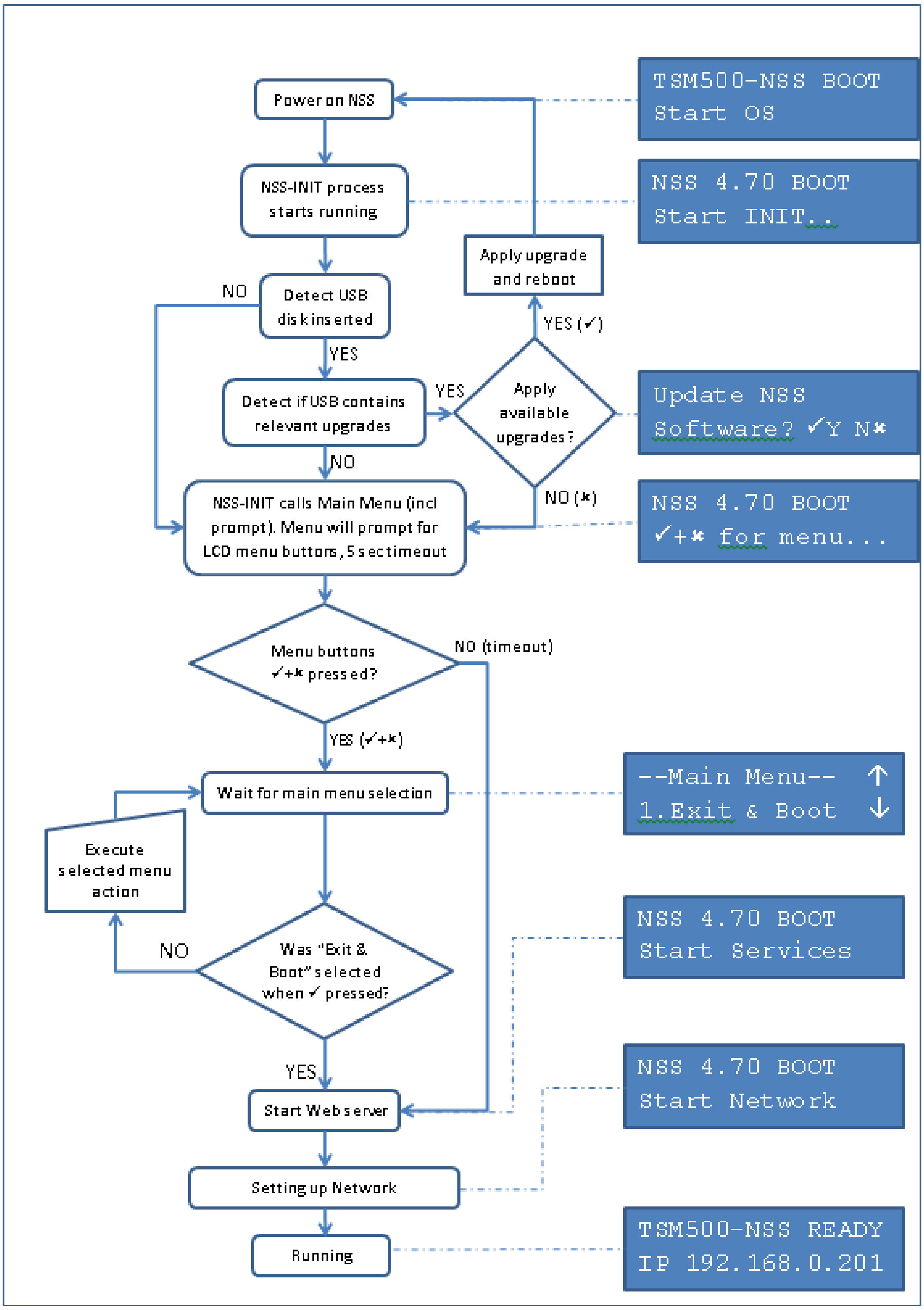
Download latest ZIP file from the FTP server e.g. NSS_v5.XX_UPDATE_REMOTE(includes xxxxx).zip. Do NOT unzip this file.

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

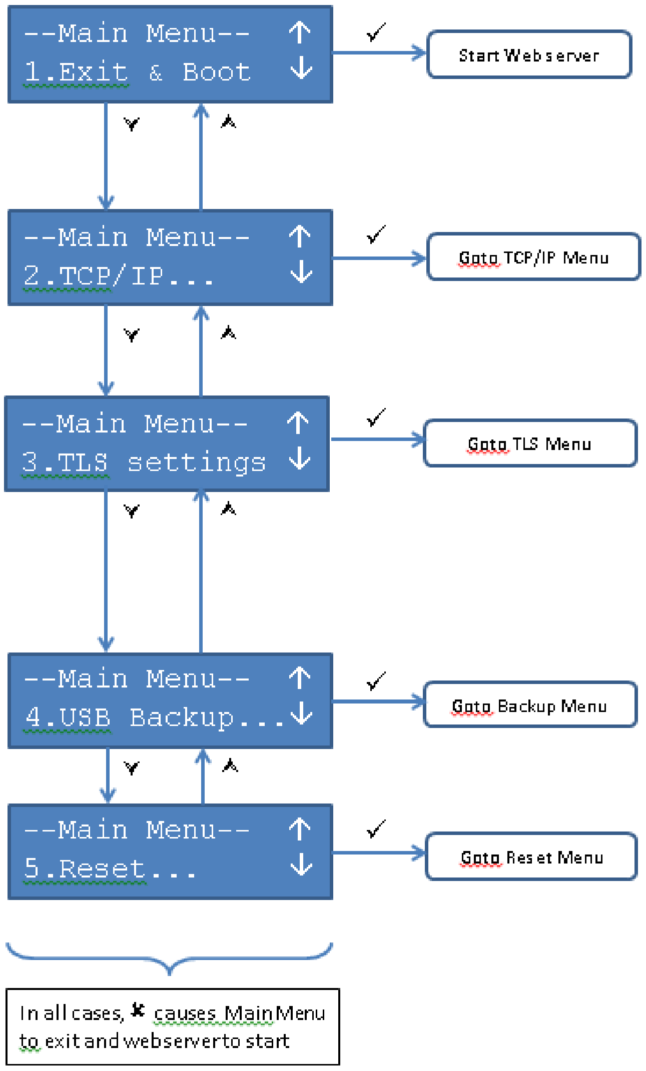
10.6 Configuring SNMP

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

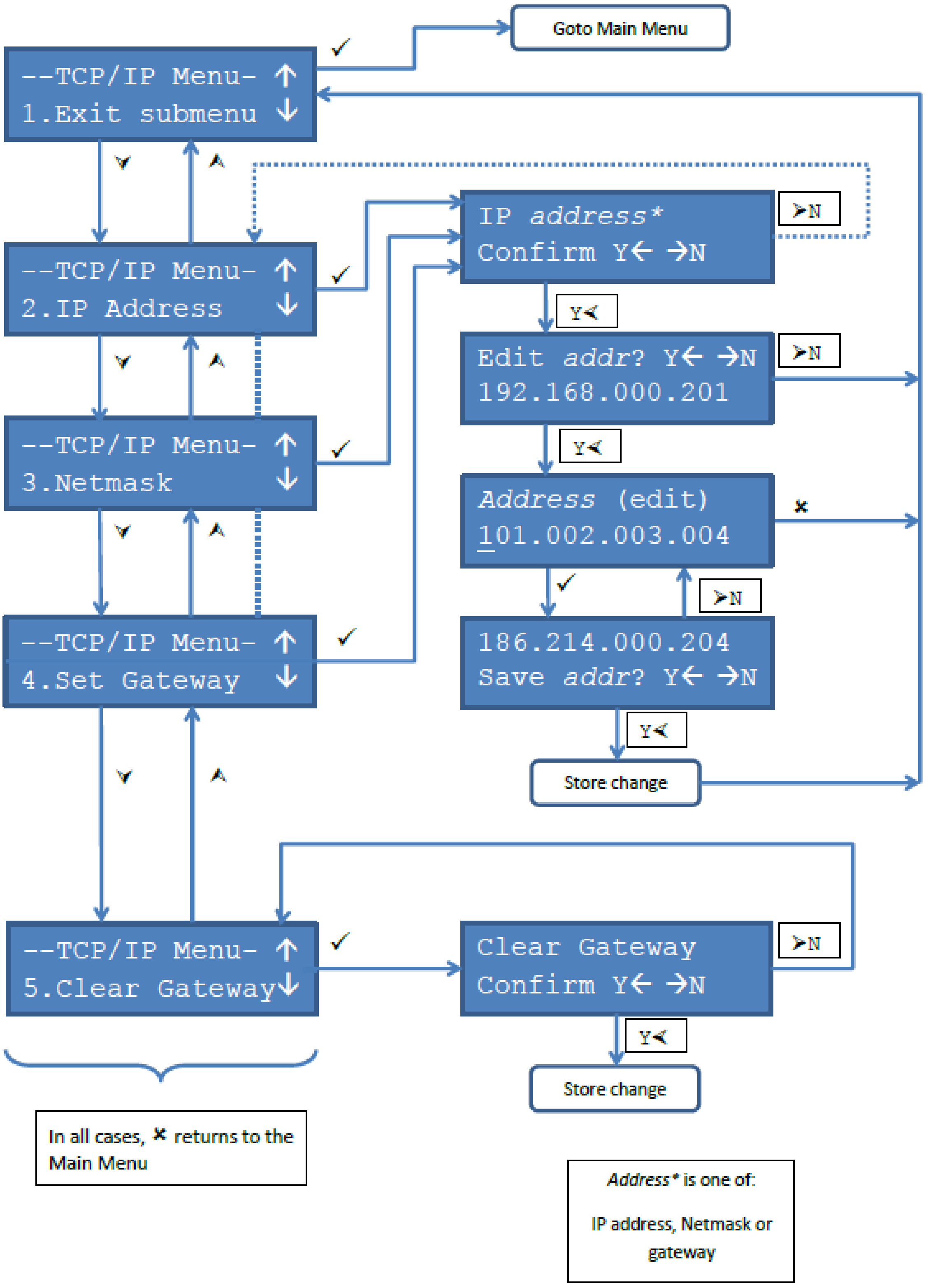
10.7 LCD Menu Sequence



Main Menu


--Main Menu-- ↑
1.Exit & Boot ↓
✓
Start Webserver
--Main Menu-- ↑
2.TCP/IP... ↓
✓
Goto TCP/IP Menu
--Main Menu-- ↑
3.TLS settings ↓
✓
Goto TLS Menu
--Main Menu-- ↑
4.USB Backup...↓
✓
Goto Backup Menu
--Main Menu-- ↑
5.Reset... ↓
✓
Goto Reset Menu
In all cases, ✗ causes Main Menu
to exit and webserver to start

TCP/IP Menu

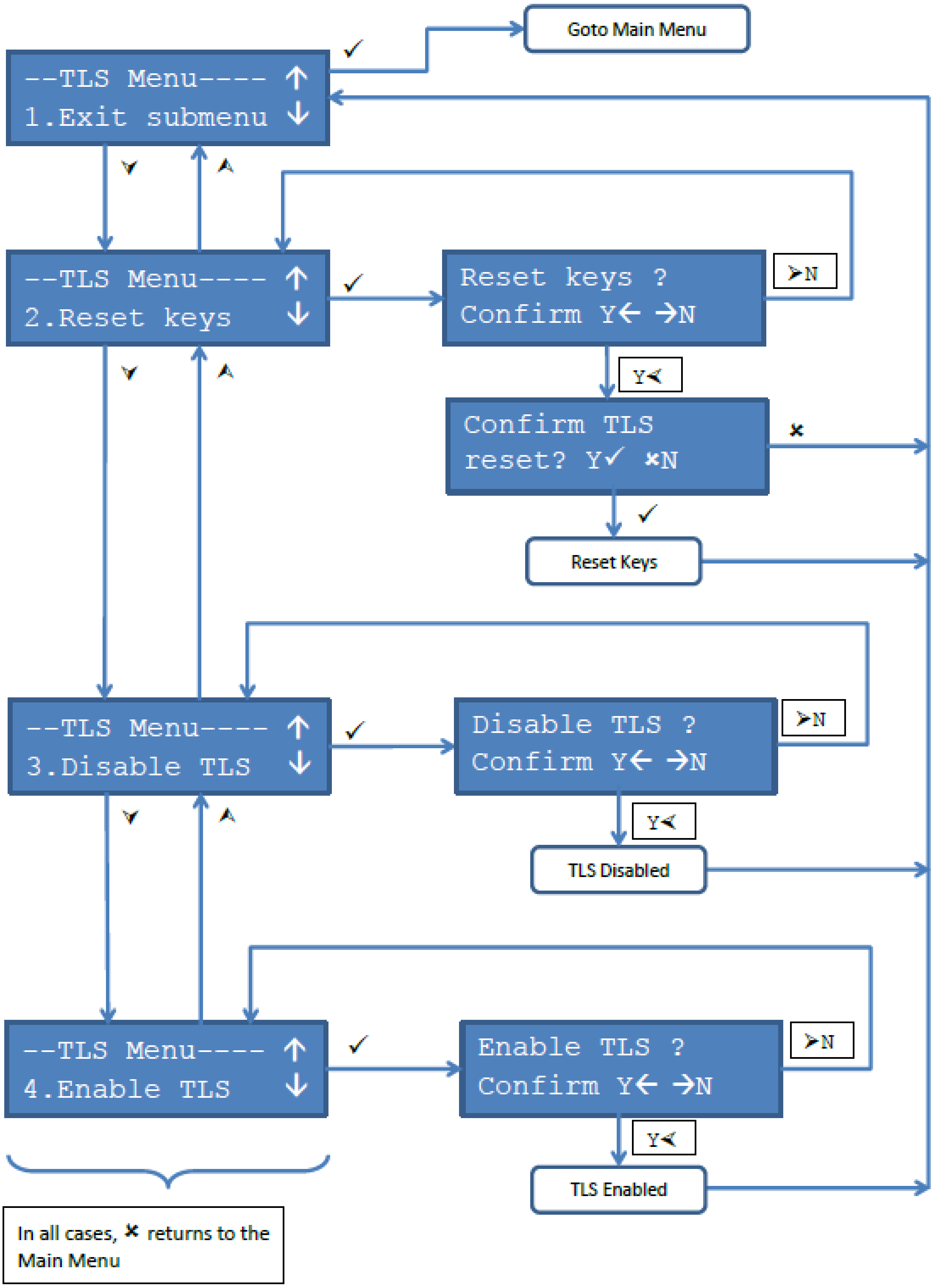


In all cases, ✗ returns to the Main Menu

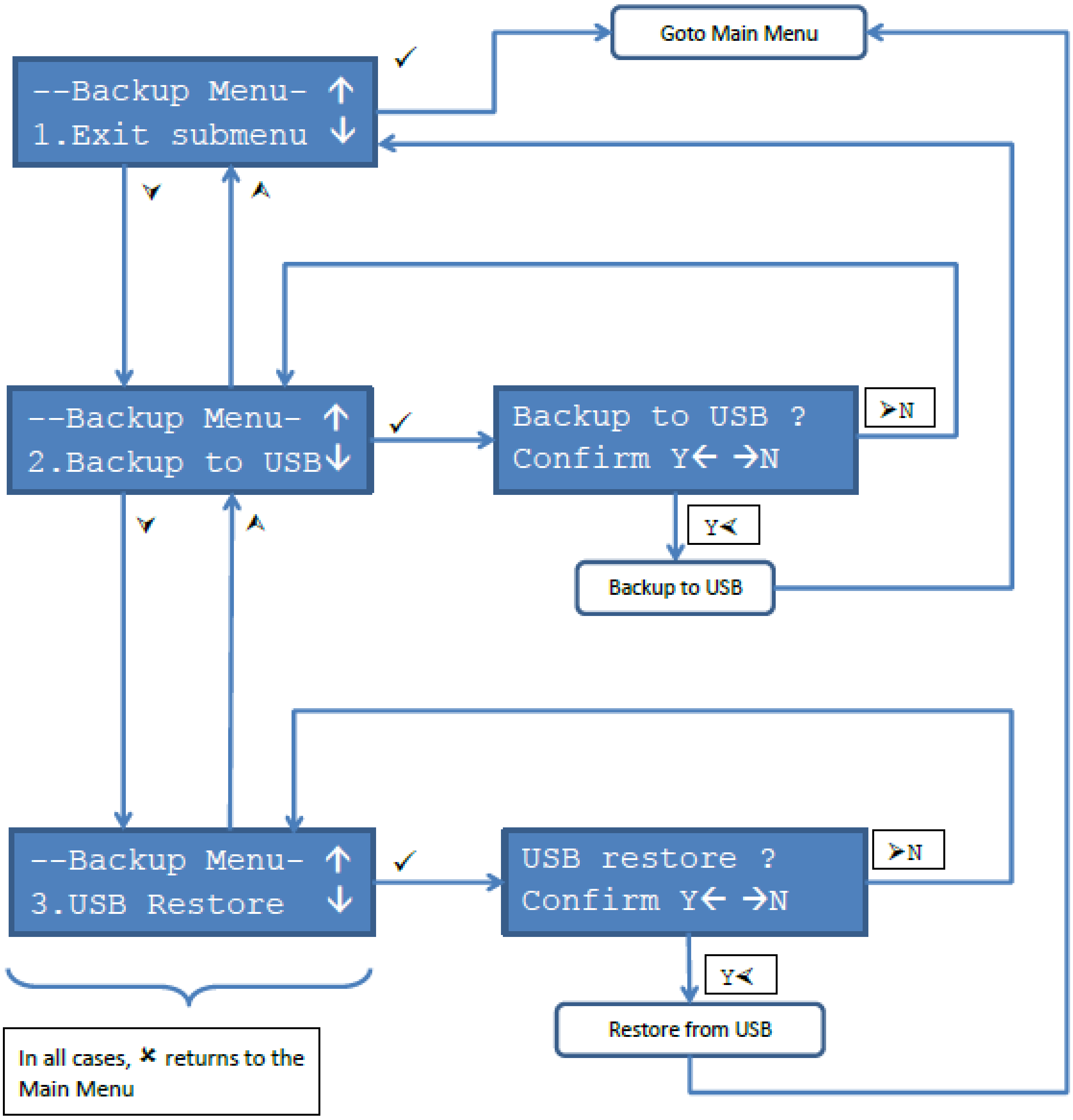
*Address** is one of:

IP address, Netmask or gateway

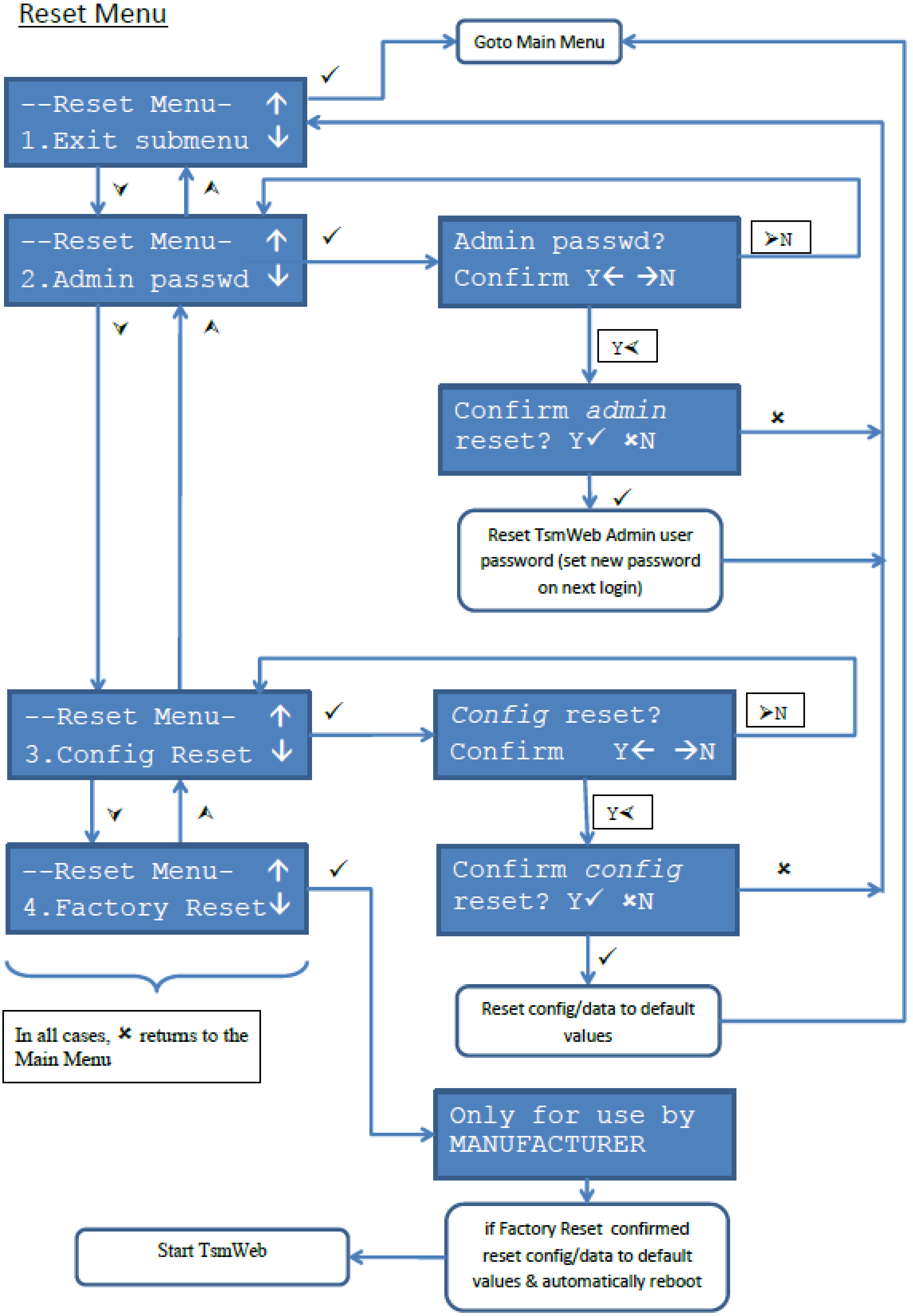
TLS Menu


Goto Main Menu
✓
--TLS Menu---- ↑
1.Exit submenu ↓
--TLS Menu---- ↑
2.Reset keys ↓
✓
Reset keys ?
Confirm Y← →N
➤N
Y≺
Confirm TLS
reset? Y✓ ✗N
✗
✓
Reset Keys
--TLS Menu---- ↑
3.Disable TLS ↓
✓
Disable TLS ?
Confirm Y← →N
➤N
Y≺
TLS Disabled
--TLS Menu---- ↑
4.Enable TLS ↓
✓
Enable TLS ?
Confirm Y← →N
➤N
Y≺
TLS Enabled
In all cases, ✗ returns to the Main Menu

Backup Menu


Goto Main Menu
--Backup Menu- ↑
1.Exit submenu ↓
--Backup Menu- ↑
2.Backup to USB↓
Backup to USB ?
Confirm Y← →N
➤N
Y➤
Backup to USB
--Backup Menu- ↑
3.USB Restore ↓
USB restore ?
Confirm Y← →N
➤N
Y➤
Restore from USB
In all cases, ✗ returns to the Main Menu

Reset Menu



In all cases, ✗ returns to the Main Menu

11 Managing Your HSM

11.1 Pairing with Secure KCED

The pairing process between the HSM and the Secure KCED is the same for a locally connected Secure KCED and the remotely connected Secure KCED. For the details on how to pair the Secure KCED with the HSM refer to sections 4.1 and 4.2.

11.2 HSM Password Management

11.2.1 How to add a Crypto Officer

⚠ **Whenever the KCED is connected to the HSM, the Cryptographic Officers must inspect the HSM, the externally connected device, and the inter-connecting cable for any signs of tampering or insertion of a bugging device.**

⚠ **If all crypto officers forget their passwords, there is NO way to reset the HSM passwords without ERASING ALL CSPs.**

This process cannot be used for setting initial passwords. Refer to section 4.3 for details on how to set passwords on initial deployment.

This process requires dual control and is therefore only possible if 2 crypto officers are able to authenticate themselves. It cannot be used where passwords have been forgotten!

Requirements:

- Logged into TsmWeb and the KCED connected to the TSM500i.
- This service can only be performed if the module is in the ***Loader*** state
- Dual authentication – two Crypto Officer must have authenticated themselves, using the KCED to login.

Process:

- Click on ***TSM > TSM Operators*** page.
- Enter the name of the new Crypto Officer in the Name field. The name must not already be in use by another operator. Click on the Add Operator button.
- The new Crypto Officer must follow the instructions displayed on the KCED. When prompted, enter the new password on the KCED, followed by a confirmation of the new password.
- A password must be at least 7 digits in length, using digits in the range 0 to 9.
- **Make a record of your password and keep in a safe place.**
- **ENSURE THAT YOU FULLY UNDERSTAND THE CONSEQUENCES OF LOSING YOUR PASSWORD!**

11.2.2 How to change an Existing Crypto Officer Password or Name

⚠ **Whenever the KCED is connected to the HSM, the Cryptographic Officers must inspect the HSM, the externally connected device, and the inter-connecting cable for any signs of tampering or insertion of a bugging device.**

⚠ **If all crypto officers forget their passwords, there is NO way to reset the HSM passwords without ERASING ALL CSPs.**

⚠ **When changing a password or name, it is required that the Crypto Officer knows the existing password and for another Crypto Officer to have authenticated themselves (dual access control).**

Requirements:

- Logged into TsmWeb and the KCED connected to the TSM500i.
- This service can only be performed if the module is in the ***Loader*** state
- Dual Authentication - two Crypto Officers must have authenticated themselves, using the KCED to login.

Process:

- Click on “Manage Operators” tab on the ***TSM > TSM Operators*** page.
- To change a password, select the appropriate *Operator ID.*
- Set the “Name” field with the details of Crypto Officer. Click on the Change Password button.
- The Crypto Officer must follow the instructions displayed on the KCED. When prompted , enter the existing password on the KCED. Then enter the new password on the KCED, followed by a confirmation of the new password.
- A password must be at least 7 digits in length, using digits in the range 0 to 9.
- **Make a record of your password and keep in a safe place.**
- **ENSURE THAT YOU FULLY UNDERSTAND THE CONSEQUENCES OF LOSING YOUR PASSWORD!**

11.2.3 Reset One Password

⚠ **Whenever the KCED is connected to the HSM, the Cryptographic Officers must inspect the HSM, the externally connected device, and the inter-connecting cable for any signs of tampering or insertion of a bugging device.**

⚠ **If all crypto officers forget their passwords, there is NO way to reset the HSM passwords without ERASING ALL CSPs.**

⚠ This operation may be used to **RESET** one password. It requires a **reset certificate from the Manufacturer** and it also requires **one Crypto Officer to authenticate themselves**.

To proceed, the customer must send a signed letter to the Manufacturer requesting the reset certificate. The letter must include the name and email address of the crypto officer that will set their password.

Requirements:

- Logged into TsmWeb and the KCED connected to the TSM500i.
- This service can only be performed if the module is in the ***Loader*** state

- One Crypto Officer must have authenticated themselves, using the KCED to login.
- Customer must have received the *Reset Password Token* for the Cryptographic Officer. These tokens will only be sent to the email specified on the signed letter. The tokens may only be **used once** where-after they will not function.

Process:

- Click on "Reset Password" tab on the ***TSM > TSM Operators*** page.
- Fill in the "Operator Name" field.
- Copy the token that was received from the Manufacturer into the box and click.
- The Crypto Officer must follow the instructions displayed on the KCED. When prompted, enter the new password on the KCED, followed by a confirmation of the new password.
- A password must be at least 7 digits in length, using digits in the range 0 to 9.
- **Make a record of your password and keep in a safe place.**
- **ENSURE THAT YOU FULLY UNDERSTAND THE CONSEQUENCES OF LOSING YOUR PASSWORD!**

11.3 Check Operational vs Privileged state

Verify that the TSM500i is in the Operational state and that it not left in the Privileged state after operations requiring dual control. The HSM will auto-logoff from the Privileged state after a pre-defined time. The time period is dependent on the type of firmware, but never exceeds 12 hours.

11.4 Upgrading TSM500i firmware

⚠ *Downgrading the firmware version or changing firmware type will result in the erasure all keys stored in the TSM500i HSM.*

A firmware upgrade of the same firmware type will preserve the keys stored in the TSM500i HSM.

⚠ *When the Crypto Officer role is required to load new firmware, all working keys will be erased*.

To upgrade TSM500i HSM firmware:

Navigate to the ***TSM > TSM Management*** page and select the "Reset TSM" tab. Click on the **Reset to Loader** button to set the TSM500i HSM to the ***Loader*** state.

One or two Crypto Officers need to authenticate with the HSM:

If loading firmware of same type and later version, the *Access Control Mode* needs to be *BL:LOADER_ROLE_**OFFICER***, i.e. one Crypto Officer needs to have authenticated with the HSM.

If loading firmware of different type or earlier version, the *Access Control Mode* needs to beBL:*LOADER_ROLE_DUAL_**OFFICER***, i.e. two Crypto Officers needs to have authenticated with the HSM.

Click on “Update Firmware” tab on the ***TSM > TSM Management*** page, browse to the file that was provided by Prism and then click on the **Update Firmware** button.

To launch the application after the firmware has been successfully loaded, select the “Reset TSM” tab click on the **Reset to App** button.

11.5 Force a tamper condition

It should only be necessary to force a tamper on an HSM when the HSM is to be decommissioned or redeployed in a different environment for a different purpose.

This service can only be performed if the module is in the ***Loader*** state and requires two Crypto Officers to have logged in.

i.e. *Access Control Mode* **must** be *BL:LOADER_ROLE_DUAL_**OFFICER***

Navigate to ***TSM > TSM Management*** page, and select the “Tamper” tab.

Click on the **Force Tamper** button to initiate the tamper condition.

This will cause the TSM500i module to reset and it will therefore be necessary to **wait** for about 20 seconds while the TSM500i initialises.

After this period, the RED LED should be ON and the GREEN LED should be flashing. This indicates that the HSM is in the Tampered state

12 Vending Tokens using PrismToken Web UI

PrismToken web UI supports the generation of:-

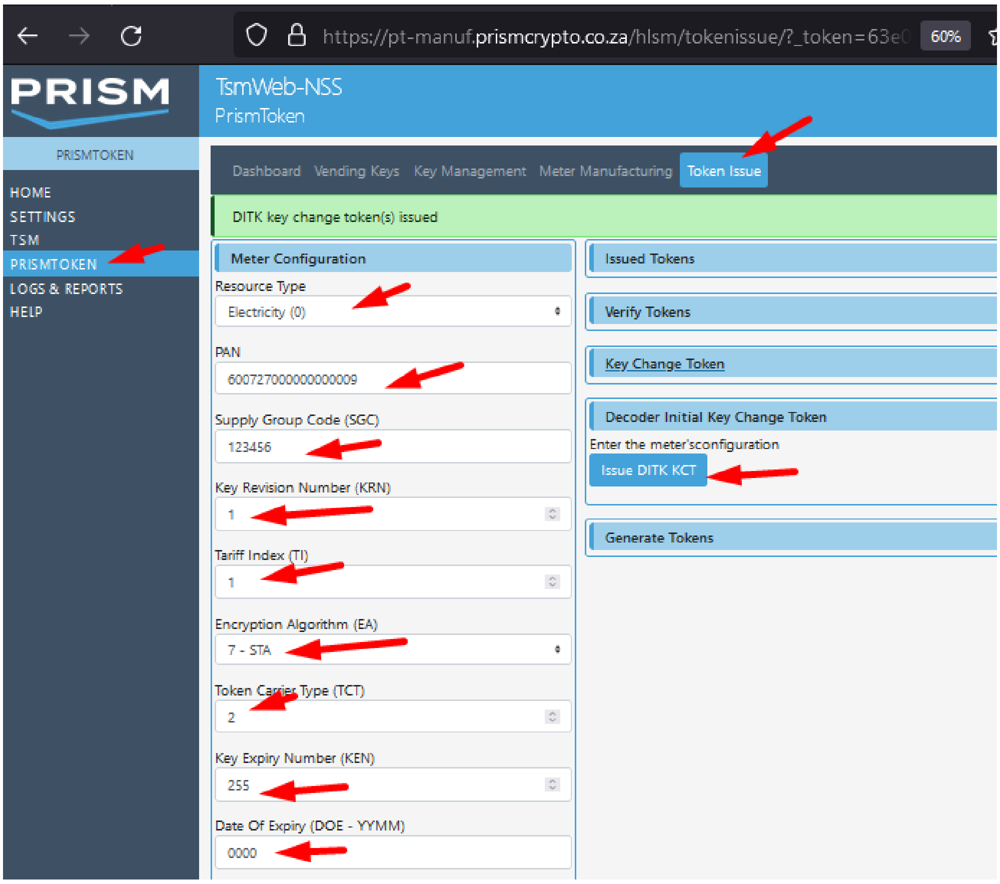
- Manufacturer Key Change tokens
- Meter Specific Engineering tokens (MSE tokens)
- STS Key Change Tokens

12.1 Manufacturer Key Change Token

Before the meter leaves the manufacturer's premises, the DITK must be replaced with a unique (DUTK), common (DCTK) or default (DDTK) key that is derived from a Vending Key.

You can use the PrismToken web User Interface (UI) to generate a set of Key Change Tokens using a dispenser ROM Key that will change a dispenser's key from the DITK to a DUTK , DDTK, or DCTK.

- Click on "PrismToken" in the left navigation menu, the select the "Token Issue" tab.
- To generate a DITK Key Change Token (for manufacturing a meter): enter the desired meter configuration (ignore the "New Meter Configuration" box), expand the "Decoder Initial Key Change" box, and click "Issue DITK KCT".



DITK key change token(s) issued

Meter Configuration

Resource Type: Electricity (0)

PAN: 6007270000000000009

Supply Group Code (SGC): 123456

Key Revision Number (KRN): 1

Tariff Index (TI): 1

Encryption Algorithm (EA): 7 - STA

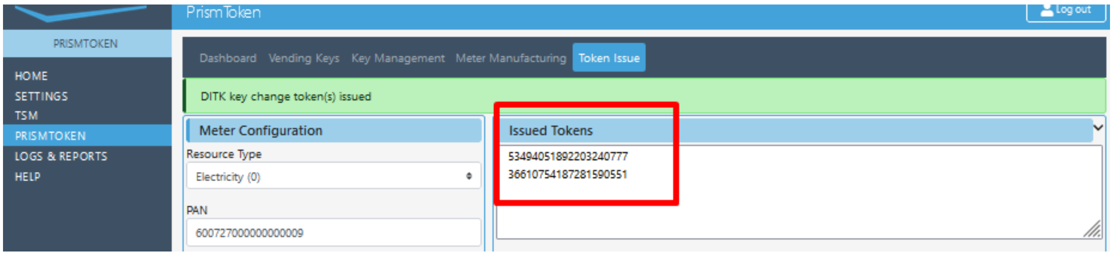
Token Carrier Type (TCT): 2

Key Expiry Number (KEN): 255

Date Of Expiry (DOE - YYMM): 0000

Decoder Initial Key Change Token

Enter the meter'sconfiguration



DITK key change token(s) issued

Meter Configuration

Resource Type: Electricity (0)

PAN: 600727000000000009

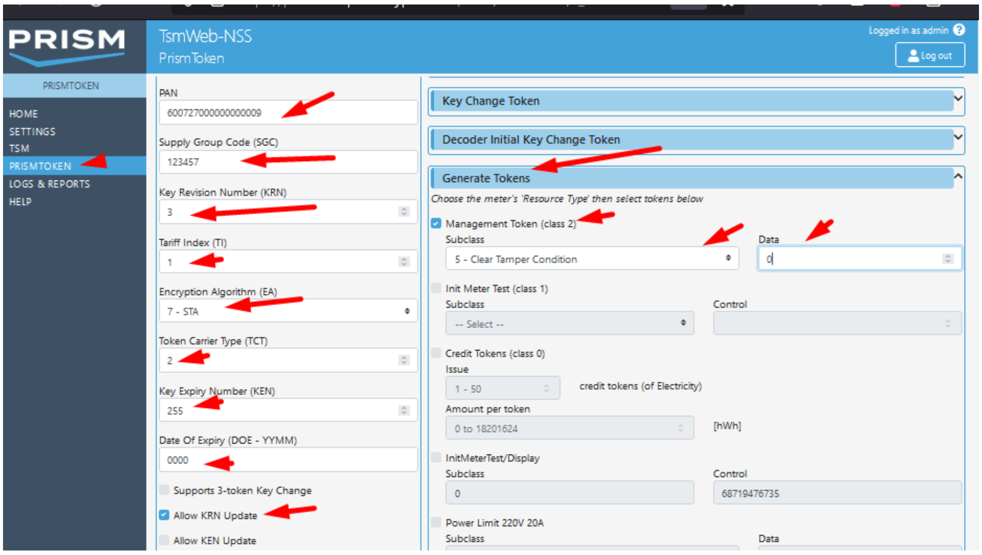
Issued Tokens

53494051892203240777
36610754187281590551

12.2 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"



PAN: 600727000000000009

Supply Group Code (SGC): 123457

Key Revision Number (KRN): 3

Tariff Index (TI): 1

Encryption Algorithm (EA): 7 - STA

Token Carrier Type (TCT): 2

Key Expiry Number (KEN): 255

Date Of Expiry (DOE - YYMM): 0000

□ Supports 3-token Key Change

☑ Allow KRN Update

□ Allow KEN Update

Choose the meter's 'Resource Type' then select tokens below

☑ Management Token (class 2)

Subclass: 5 - Clear Tamper Condition | Data: 0

□ Init Meter Test (class 1)

Subclass: -- Select -- | Control:

□ Credit Tokens (class 0)

Issue: 1 - 50 credit tokens (of Electricity)

Amount per token: 0 to 18201624 [hWh]

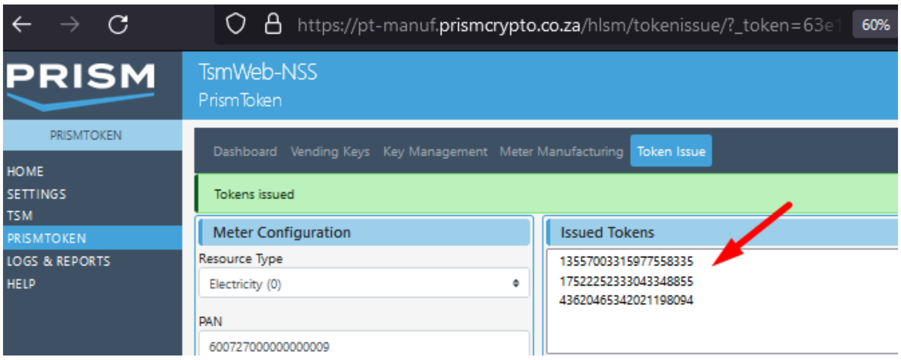
□ InitMeterTest/Display

Subclass: 0 | Control: 68719476735

□ Power Limit 220V 20A

Subclass: | Data:

- 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.



Tokens issued

Meter Configuration

Resource Type: Electricity (0)

PAN: 600727000000000009

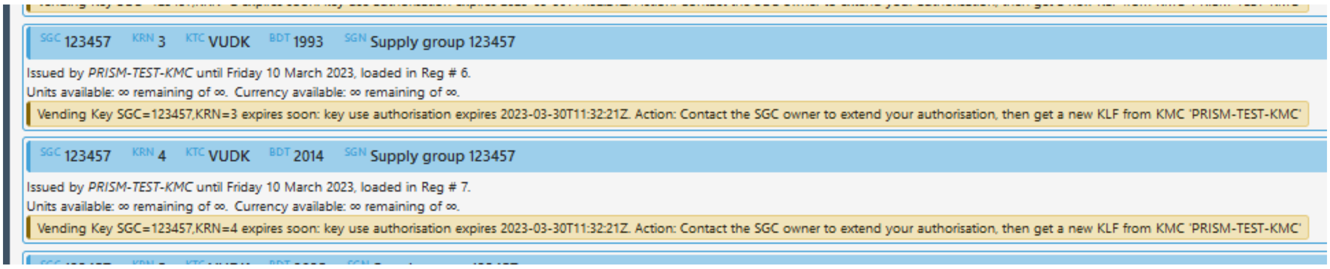
Issued Tokens

13557003315977558335
17522252333043348855
43620465342021198094

12.3 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.



SGC 123457 KRN 3 KTC VUDK BDT 1993 SGN Supply group 123457

Issued by *PRISM-TEST-KMC* until Friday 10 March 2023, loaded in Reg # 6.
Units available: ∞ remaining of ∞. Currency available: ∞ remaining of ∞.

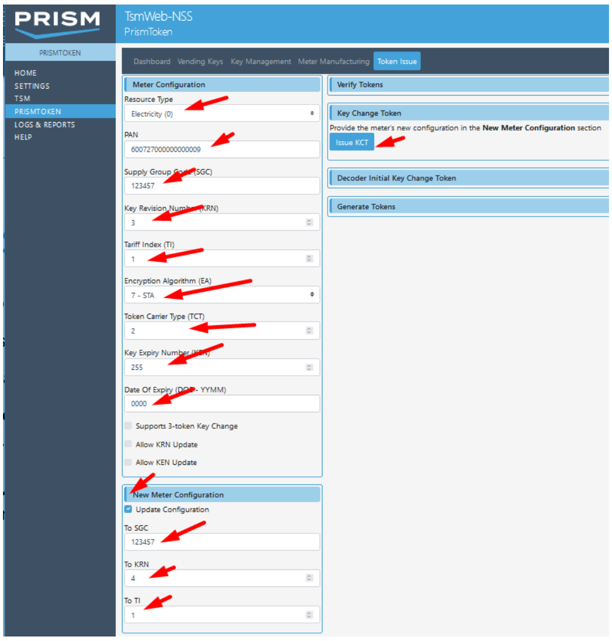
Vending Key SGC=123457,KRN=3 expires soon: key use authorisation expires 2023-03-30T11:32:21Z. Action: Contact the SGC owner to extend your authorisation, then get a new KLF from KMC 'PRISM-TEST-KMC'

SGC 123457 KRN 4 KTC VUDK BDT 2014 SGN Supply group 123457

Issued by *PRISM-TEST-KMC* until Friday 10 March 2023, loaded in Reg # 7.
Units available: ∞ remaining of ∞. Currency available: ∞ remaining of ∞.

Vending Key SGC=123457,KRN=4 expires soon: key use authorisation expires 2023-03-30T11:32:21Z. Action: Contact the SGC owner to extend your authorisation, then get a new KLF from KMC 'PRISM-TEST-KMC'

- 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.



Meter Configuration

Resource Type: Electricity (0)

PAN: 6007270000000000009

Supply Group Code (SGC): 123457

Key Revision Number (KRN): 3

Tariff Index (TI): 1

Encryption Algorithm (EA): 7 - STA

Token Carrier Type (TCT): 2

Key Expiry Number (KEN): 255

Date Of Expiry (DOE - YYMM): 0000

□ Supports 3-token Key Change

□ Allow KRN Update

□ Allow KEN Update

New Meter Configuration

☑ Update Configuration

To SGC: 123457

To KRN: 4

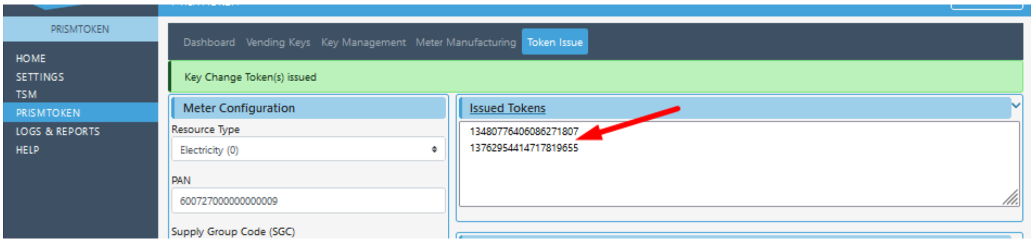
To TI: 1

Key Change Token

Provide the meter's new configuration in the **New Meter Configuration** section

Issue KCT

- 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 6007270000000000009 if it has been configured on SGC 123457, KRN 3, TI 1.



Key Change Token(s) issued

Meter Configuration

Resource Type: Electricity (0)

PAN: 6007270000000000009

Supply Group Code (SGC)

Issued Tokens

13480776406086271807
13762954414717819655

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