Tel: +27 11 343 2000 | **Fax**: +27 11 442 5908 | **Email**: info@prism.co.za
Address: President Place, Johannesburg, South Africa

Payments TSM500i NSS User Guide (PCI HSM v3)

December 2022

Document number:	PR-D2-1123 Rev 1.0
Release date:	December 2022
Copyright:	
Synopsis:	This document describes the PCI HSM v3.0 Payments TSM500i-NSS Hardware Security Module (HSM), with Common (COM) API and/or MCM API, as well as the TsmWeb interface used to manage this HSM.

Company Confidential

Disclaimer

Tel: +27 11 343 2000 | **Fax**: +27 11 442 5908 | **Email**: info@prism.co.za
Address: President Place, Johannesburg, South Africa

Important Notes

This document only applies to a 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.

Do NOT use the TSM500i without first following all of your organisation's established security procedures so that it is commissioned in accordance with PCI DSS and/or PCI P2PE requirements. Section 2 provides a flow chart as a quick guide for the process from installation to operation.

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 4.2. 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

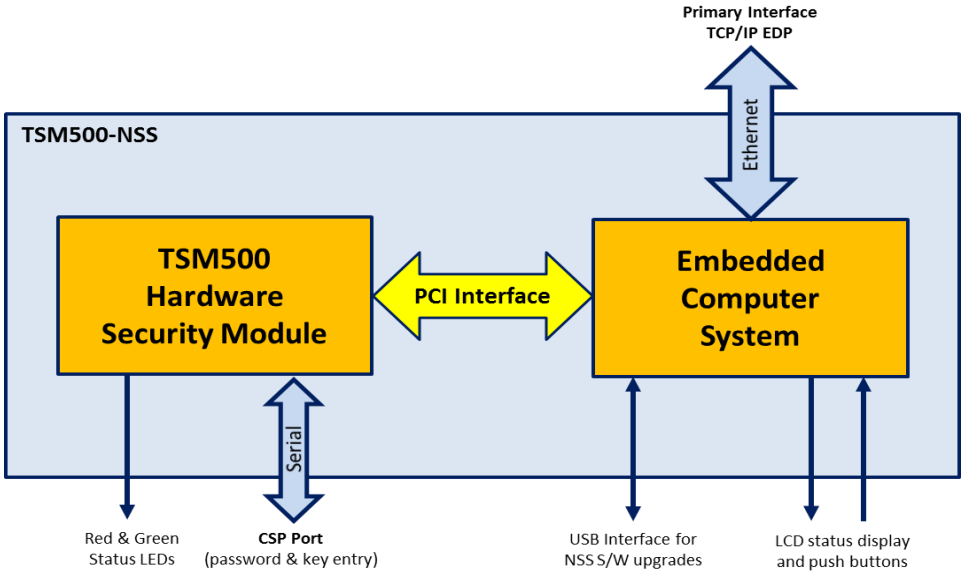
1 Overview

The TSM500i 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 a TSM500i that has Boot Loader v1.5.0.0 or later.**

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.



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 Key Components
- Generation of Key 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.

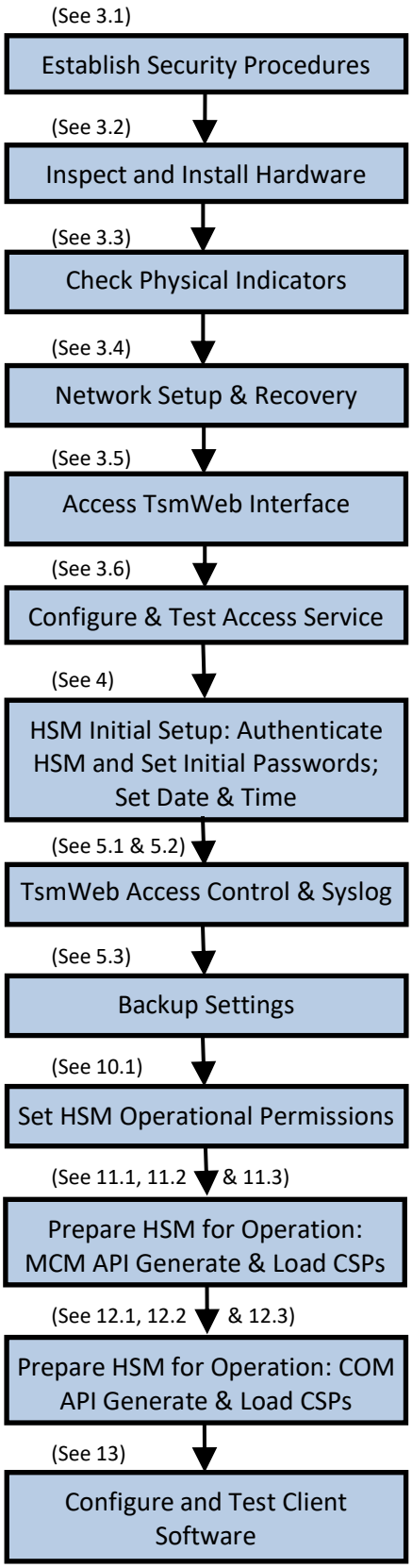
TSM500i LEDs **USB PORT (NSS software updates and KCED)**

Hardware version: 5520-00130_v1.2_NSS

The KCED when used locally connects directly to the TSM500i HSM (Hardware version:5520-00130_v1.1_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



The TSM500i and its Critical Security Parameters (CSPs) must be handled in accordance with documented security procedures in order to meet the security requirements of the Banking Industry and standards bodies. Refer to ***Sample Security producedure.pdf***

The TSM500i NSS hardware must be inspected and then installed in a secure environment in accordance with the procedures detailed in this User Guide

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.

Configure and test access service according to the HSM API

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*.*
If required, the date and time can be set to match your time zone

Setup TsmWeb access control by creating TsmWeb user accounts and set account expiry dates, setting the password policy and default auto-logoff times
Setup Syslog publishing

Follow the backup procedure to backup TsmWeb settings

If required, additional TSM500i HSM operational permissions should be set at this point

If using MCM API: CSPs must be loaded into the TSM500i HSM to configure it for operational use. The most important CSP is usually the Storage Master Key (SMK), which is split between several custodians in the form of components. If required, additional TSM500i HSM operational permissions can be set at this point

If using Common API: CSPs must be loaded into the TSM500i HSM to configure it for operational use. The most important CSP is usually the Storage Master Key (SMK), which is split between several custodians in the form of components. If required, additional TSM500i HSM operational permissions can be set at this point.

Client software must be configured to communicate with appropriate access service, which depends on the API being used. Testing needs to be to ensure that transaction processing can proceed successfully. Third-party tools will be used during this step.

3 NSS Initial Setup

3.1 Establish Security Procedures

Security procedures that monitor and control access to the environment, the HSMs and the Critical Security Parameters (CSPs) must be documented and put in place.

FIPS, PCI, the Banking Industry and Card Institutions mandate such procedures.

You will need to create your own security procedures that are appropriate for your industry, environment and hardware.

ⓘ Detailed recommendations for creating your own procedures that are suitable for the retail banking industry can be found in *Sample Security Procedures.pdf* (Doc. PR-D2-0621).

Both VISA and MasterCard provide audit compliance guidelines that are a good reference for creating security procedures. A valuable source of information is the *PCI PIN Security Requirements*.

At minimum the following issues should be addressed:

- The environment containing TSMs should be physically secure, with logged access control.
- There should be periodic inspections to check compliance with security procedures.
- A procedure for commissioning a new HSM, including checking that it has been received intact, assignment of administrators or responsible individuals, and storage of management passwords.
- A procedure for loading CSPs, including requirements for selecting custodians, generating the Storage Master Key (SMK), and storing SMK components.
- A procedure for backing up critical data, including the SMK, Key Space configuration, and the key database.
- A procedure for maintenance, which must ensure that CSPs in the HSM are destroyed before it is removed from the secure environment.
- A procedure for decommissioning, which must ensure that CSPs in the HSM are destroyed.

3.1.1 Security Awareness, and the implication of lost passwords and/or components

The following example is used to highlight the importance of security awareness and the implication of lost passwords and components:

In an organisation Andy has the administrative (Admin) role for an HSM. Andy "owns" or is responsible for the HSM. Ben and Collin are the designated crypto officers for the HSM. Don and Eric are the designated key custodians for the HSM.

The organisation will need to consider the following scenarios:

- **If <u>both</u> Ben and Collin (i.e. <u>both</u> crypto officers) <u>forget</u> their passwords then it will not possible to reset their passwords without erasing all keys.**

- **If either Ben or Collin (i.e. one crypto officer) forgets their passwords, it will not be possible to perform any operation that requires dual authentication on the HSM, such as loading key components. The client will have to request a password reset certificate from Prism (on behalf of the officer who forgot their password).**
- **If either Ben or Collin (i.e. one crypto officer) resigns from the organisation, and forgets to handover their password, it will not possible to reload the key onto the current HSM, or load the key onto new HSMs. The client will have to request a password reset certificate from Prism (on behalf of the officer who resigned).**
- **If either Don or Eric (i.e. one key custodian) forgets their key components, it will not be possible to reload the key onto the current HSM, or load the key onto new HSMs.**
- **If either Don or Eric (i.e. one key custodian) resigns from the organisation, and forgets to handover their key component, it will not be possible to reload the key onto the current HSM, or load the key onto new HSMs.**

For the above mentioned reasons, the client needs to be aware of the following:

- It is critical to assign someone who "owns" or is responsible for the HSM.
- This person has the administrative (Admin) role and it responsible for managing personnel changes for themselves, Crypto Officers and Custodians.
- They should manage a key register which details of who the custodians are and where the components are stored
- They should manage a crypto officer register which details who the crypto officers are and where their passwords are stored.
- Any changes need to be recorded so that the registers are kept up to date
- A minimum of two crypto officers are required, but it is highly recommended that three crypto officers be assigned.
- It is highly recommended that Crypto Officers securely store their passwords.
- It is highly recommended that Custodians securely store their component(s).
- The Administrator, Crypto officers and Custodians should perform a security awareness training exercise by going through the security procedures that apply to them in the sample security procedures guide

Please read through the following sections of the Sample Security Procedures document:

- Section 4 of the sample security procedures document
- Annex F Key Register
- Annex H Security Awareness Training Form

3.2 Inspect and Install Hardware

3.2.1 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.

3.2.2 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".

3.3 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)

3.4 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 3.4.1). 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.

3.4.1 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.

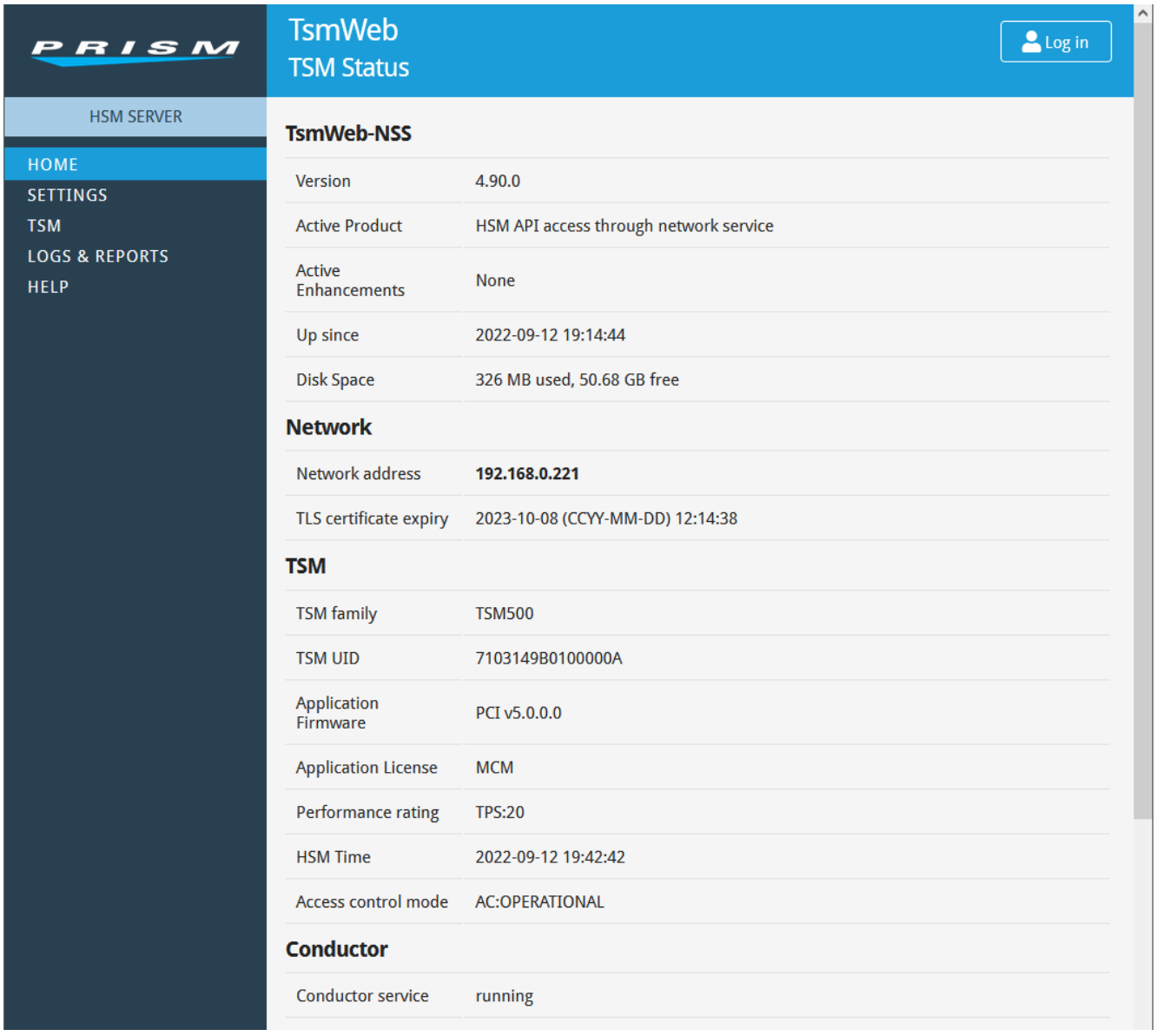
More details about the MAIN MENU can be found in section 8.7.

3.5 TsmWeb Interface

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

3.5.1 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).



3.5.2 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.

3.5.2.1 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.

3.5.3 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 3.5.2 and 5.1 for details on how to setup a TsmWeb admin password and further user passwords.

3.5.4 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**.

3.6 Configuring & Test Access Service

3.6.1 Configuring Conductor Service on the TSM500i-NSS

This section is not applicable to HSMs with Common API firmware HSM.

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.

3.6.1.1 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.

3.6.1.2 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.

3.6.1.3 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.

3.6.1.4 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.

3.6.2 Configuring Common API Service on the TSM500i-NSS

This section is not applicable to HSMs with MCM API firmware HSM.

It is not usually necessary to configure HSM Server on the TSM500i-NSS. The default settings will work in most environments. TsmWeb allows the user to manage the HSM Server configuration TCP port, header length and character set via the ***TSM > Common API*** dashboard page.

Accessing HSM Server from a different subnet through a firewall appliance will require that that the HSM Server TCP Port (default 1500) is enabled for incoming connections on the firewall.

3.6.2.1 Changing the TCP Port, Header Length or Character Set

From the ***TSM > Common API*** dashboard page click on the ≡ TASKS button on the "Server Configuration" pane. Edit the Port, Header Length and/or Character Set values then clicking on **Change** button to effect the change.

3.6.2.2 Changing the Log Level

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

To enable debug level tracing of Common API calls in a test/UAT environment set each of the preferences listed below as follows:

com.server.log_io_level=verbose

com.server.log_level=verbose

tsmwebinit.loglevel=verbose

To change each preference, click on the Edit link in the corresponding table row, edit the Current Value and click the **Set** button.

The NSS needs to be rebooted for the changes in log level to become active. To reboot the NSS with TsmWeb navigate to the ***Settings > System*** page and click the **Reboot NSS** button. Alternatively the NSS can be powered off and then back on again.

In production environment the log levels would typically be set to the following values

com.server.log_io_level=err

com.server.log_level=warn

tsmwebinit.loglevel=info

3.6.2.3 Setting the Maximum Log File Sizes

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

com.server.log_maxsize (default = 512000 and the minimum is 64000)

tsmwebinit.log.maxlogsize (default = 3072000 and the minimum is 64000)

To change each preference, click on the Edit link in the corresponding table row, edit the Current Value and click the **Set** button.

Care should be taken to not set the log file so large so that there is insufficient space for the all the x-comsvcio.X.txt and tsmweb.X.txt logfiles.

The available disk space can be viewed on the TsmWeb home page.

4 HSM Initial Setup

4.1 Pairing the TSM500i HSM with the Secure KCED

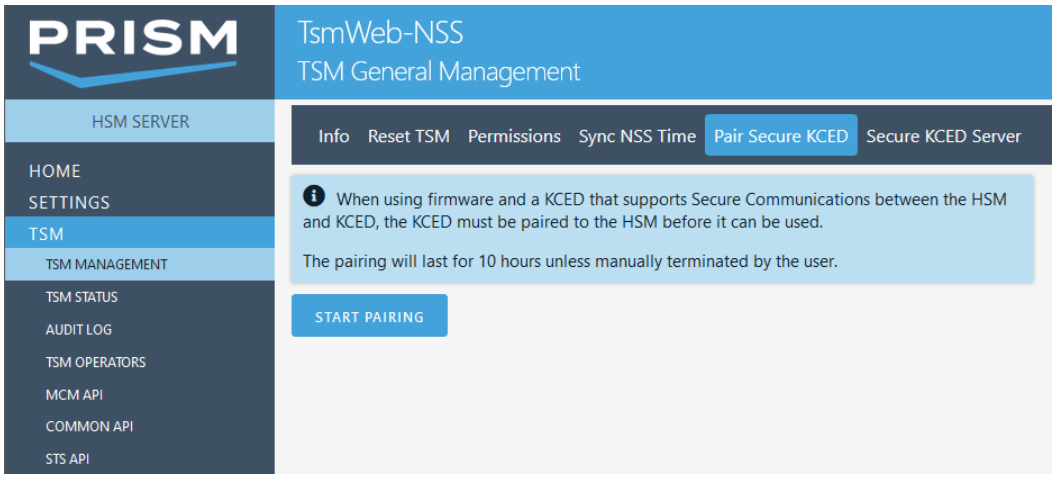
TSM500i HSMs shipped with V1.6.0.0 (or later) Boot loader and V5.0.0.0 (or later) Application firmware must be paired with a Secure KCED, before the Secure KCED can be used to setup Crypto Officers, to display generated components or be used for key component entry.

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.

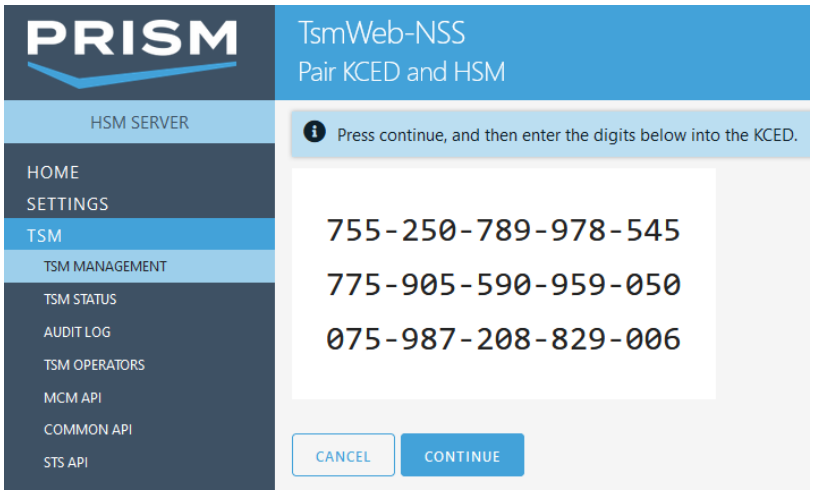
Connecting the KCED after powering it on will result it not being able to communicate with the HSM.

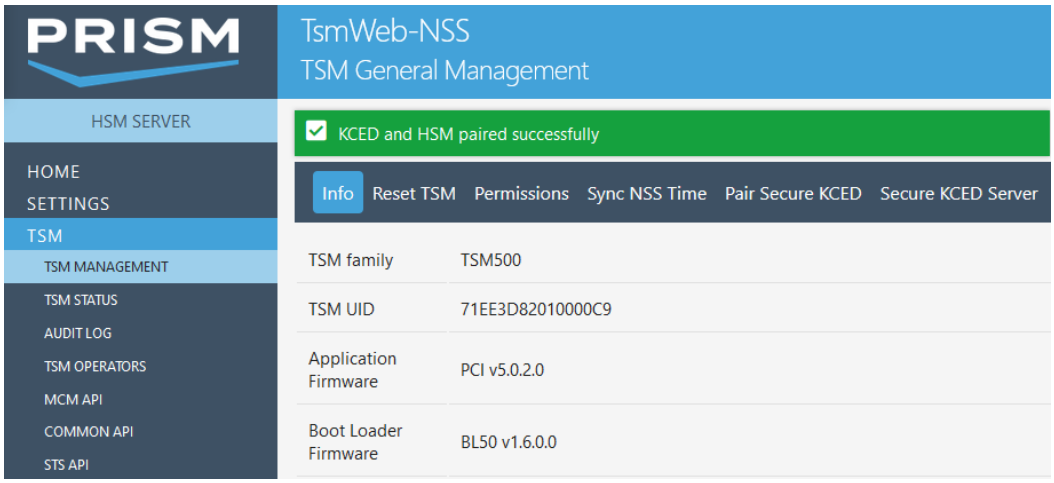
To pair the KCED with the HSM navigate to ***TSM > TSM Management***, and select the "Pair KCED" tab.



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.





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.

4.2 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.

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 Add additional crypto officers

Refer to section 9.3.1 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.

4.3 [Optional] Set Date and Time

4.3.1 Set Date and Time

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

Prism sets the date and time on the TSM500i HSM system to UTC +2 hours which is the local time where the hardware is manufactured. In the case of a TSM500i-NSS, the same date and time is applied to the clock of the embedded computer.

Setting the TSM500i-NSS date and time will result in the embedded computer system time also being set so that both stay synchronised. The TSM500i-NSS does not support daylight saving time.

The HSM's date and time is a Critical Security Parameter for certain cryptographic functions, and should be corrected at this point.

This service requires two Crypto Officers to login to the TSM500i HSM using the KCED.

i.e. *Access Control Mode* **must** be *BL:ROLE_**DUAL_OFFICER***

In the browser on the ***TSM > TSM Management*** page click on "Date and Time" tab. Enter the correct date and time using the format indicated on the page then click **Set Clock** to update the date and time in the TSM500i HSM and the embedded computer system.

4.3.2 Put the TSM500i back into the Application Running State

To change from the ***Loader*** state back to ***Operational*** state (only possible if the Loader is not in the Tampered or Error state), click on "Reset TSM" tab on the ***TSM > TSM Management*** page. Click on **Reset To App** and allow about 20 seconds (until green LED is flashing) for the TSM500i module to complete its initialisation before attempting to communicate with it again.

5 TsmWeb Initial Setup

5.1 Setup TsmWeb Access Control

When using a TSM500i-NSS in an EFT payment system or key injection solution for terminals, TsmWeb access control needs to be configured so that it complies with PCI-DSS security requirements. The details of PCI-DSS security requirements are beyond the scope of this guide and the user should refer to the latest PCI-DSS security requirements from the PCI Security Standards Councils website.

5.1.1 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

5.1.2 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.**

5.1.3 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.

5.1.4 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'.

5.2 Enable Syslog Publishing

Refer to TSM500i-NSS Syslog Application Note (PR-D2-1122) for details on how to enable Syslog publishing to a SIEM server.

5.3 Backup NSS Settings

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

- Power the TSM500i-NSS off.
- Insert a USB flash drive (NTFS preferred, FAT32 supported) into the USB port on the front panel of the TSM500i-NSS.
- Power it on again and hold down the red ✗ button and green ✓ button on the TSM500i-NSS front panel until the MAIN MENU appears on the LCD display. Refer to section 8.7 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".

6 Status & Diagnostics

6.1 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.

6.2 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.

6.3 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 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

6.4 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.

6.5 Look at the LCD

If you cannot communicate with TsmWeb, Conductor or the HSM Server waiting for the TSM500i-NSS to 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.

6.6 TSM500i Status LEDs

After powering on the TSM500i-NSS check status LEDs that are located on the front panel. Refer to section 3.3 for description of the LED states.

6.7 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.

7 Managing TsmWeb

7.1 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 2 years. 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 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.

7.1.1 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.

7.1.1.1 Disable or Enable TLS from TsmWeb

To enable or disable TLS via TsmWeb, navidate 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.

7.2 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 5.3) all the preferences are included in the backup.

8 Managing Your NSS

8.1 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 3.4.1 or section 8.7.

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 8.3.1
- Set IP Address, Netmask, default gateway - refer to section 3.4.1
- USB Backup & Restore - refer to section 5.3
- Reset to Defaults - refer to section 8.3
- Disable SSL/TLS, reset TLS key - refer to section 7.1.1

8.2 Backup and Restore

8.2.1 Backup & Restore on a TSM500i-NSS

Backup

Refer to section 5.3 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 section 8.7 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 (8.1) 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.

8.3 Reset NSS to Default Settings

Section 8.1 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:

8.3.1 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 3.5.2.1.

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 3.5.2.1.

8.3.2 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")

8.3.3 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".

8.4 Disable TLS from the LCD MENU

Using the LCD MAIN MENU as described in section 8.1, select the "Disable TLS" option and confirm the operation. The TLS service is now disabled.

8.5 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.

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.

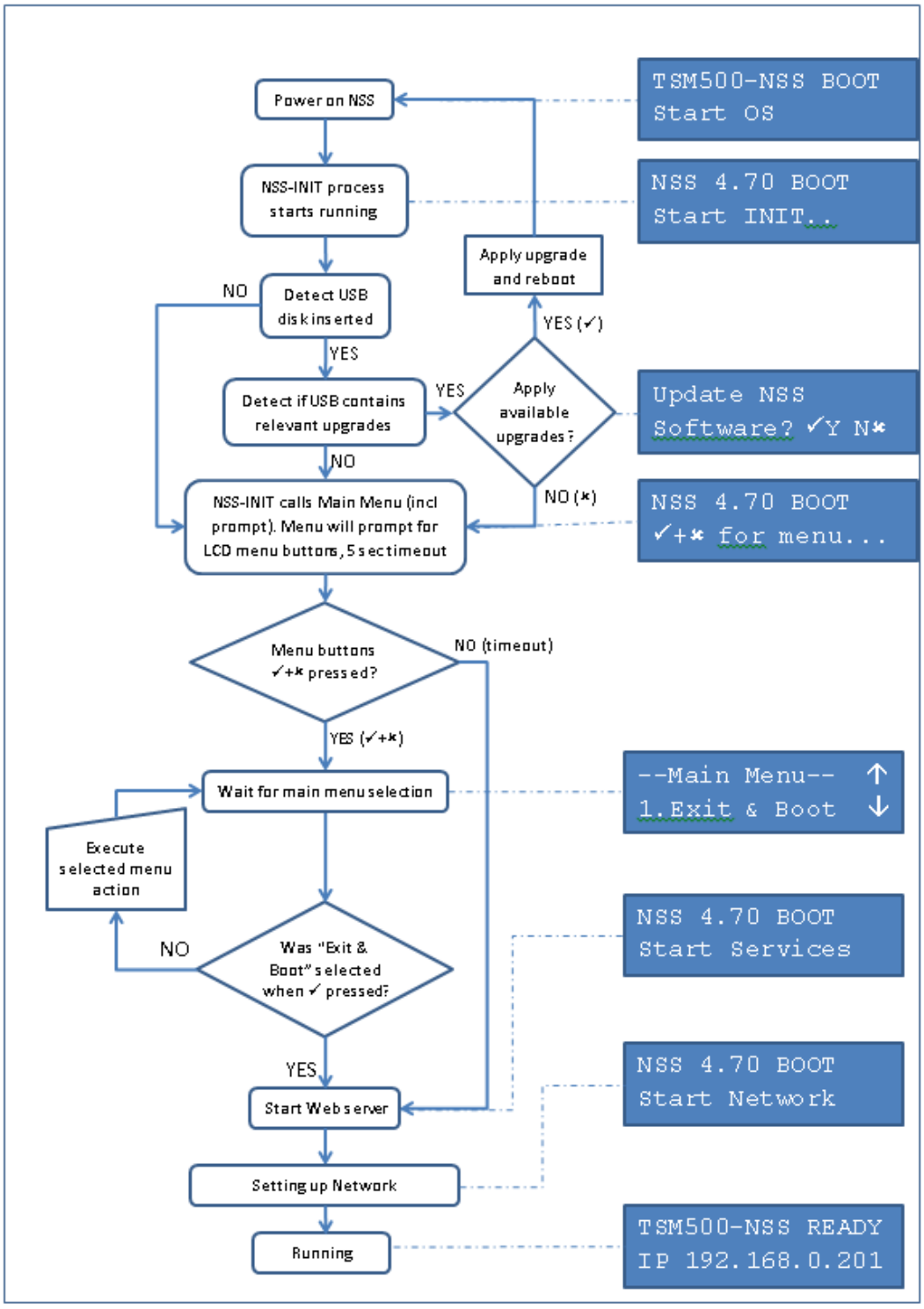
Special requirement: upgrading from versions before NSS v4.75

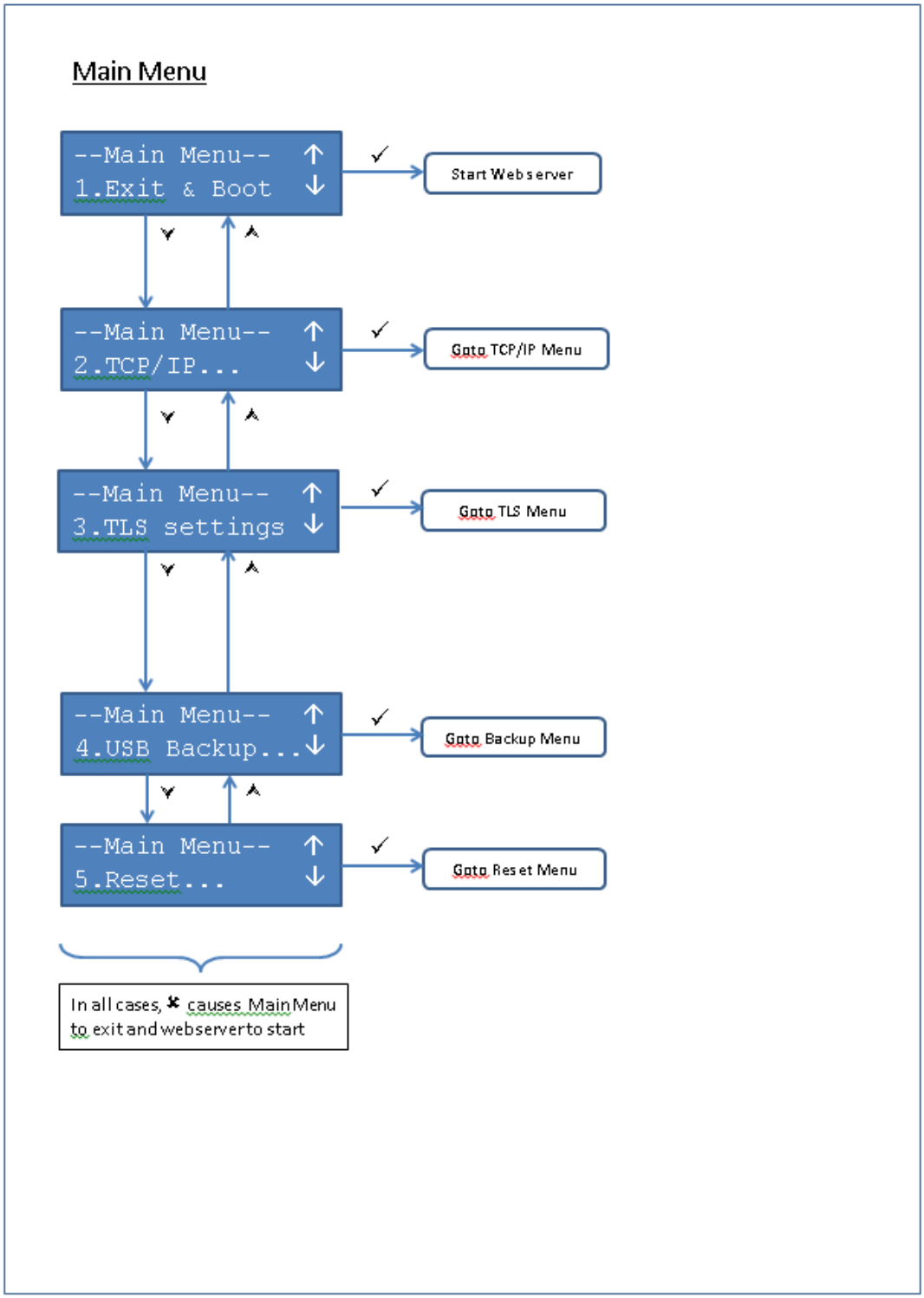
NSS v4.75 introduces a new database structure that improves disk space utilization. The process of upgrading to v4.75 (or higher) includes a mandatory and automatic backup, plus a database migration (that is performed via an automatic restore). The USB flash drive that contains the NSS_UPDATES directory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

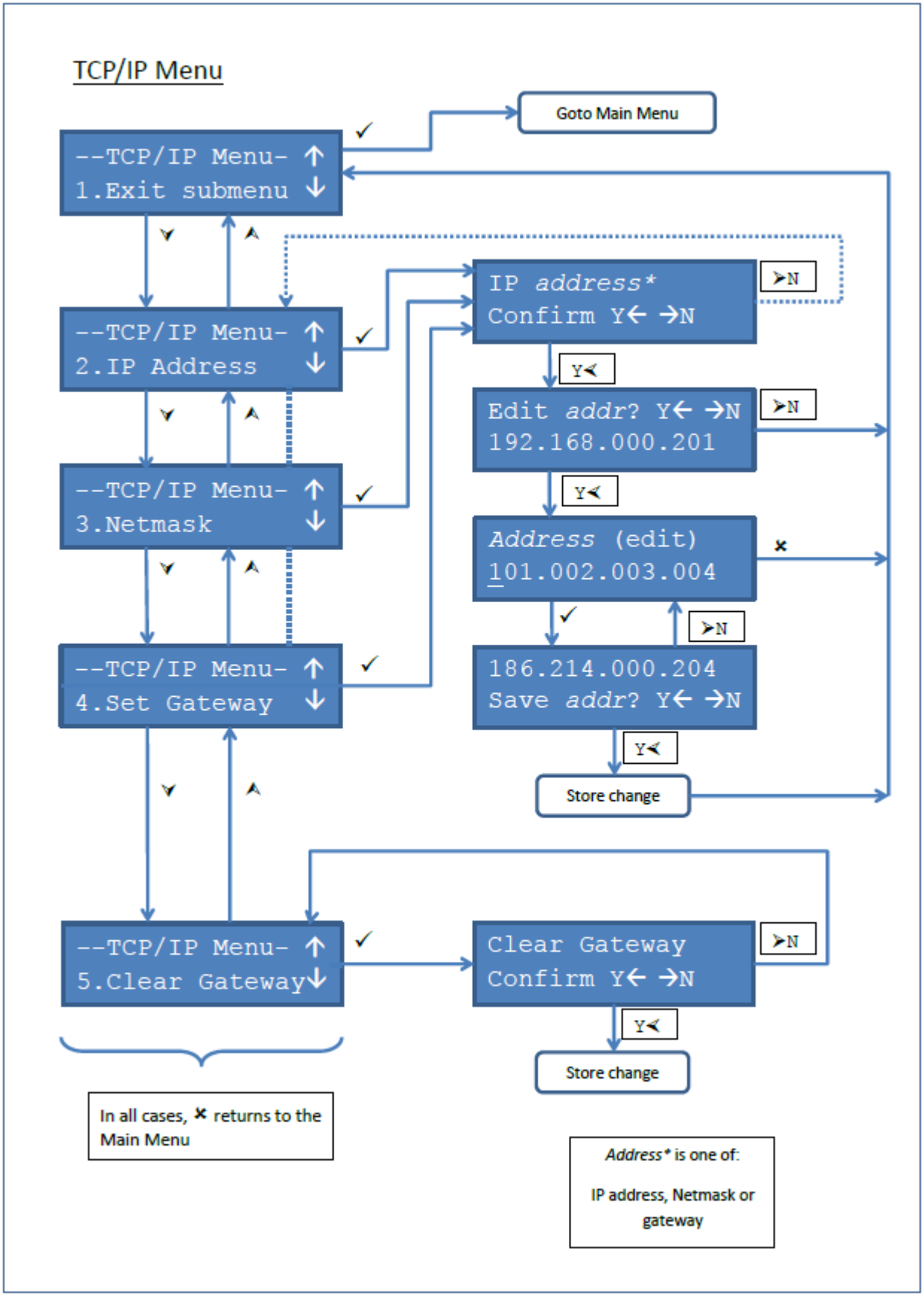
8.6 Configuring SNMP

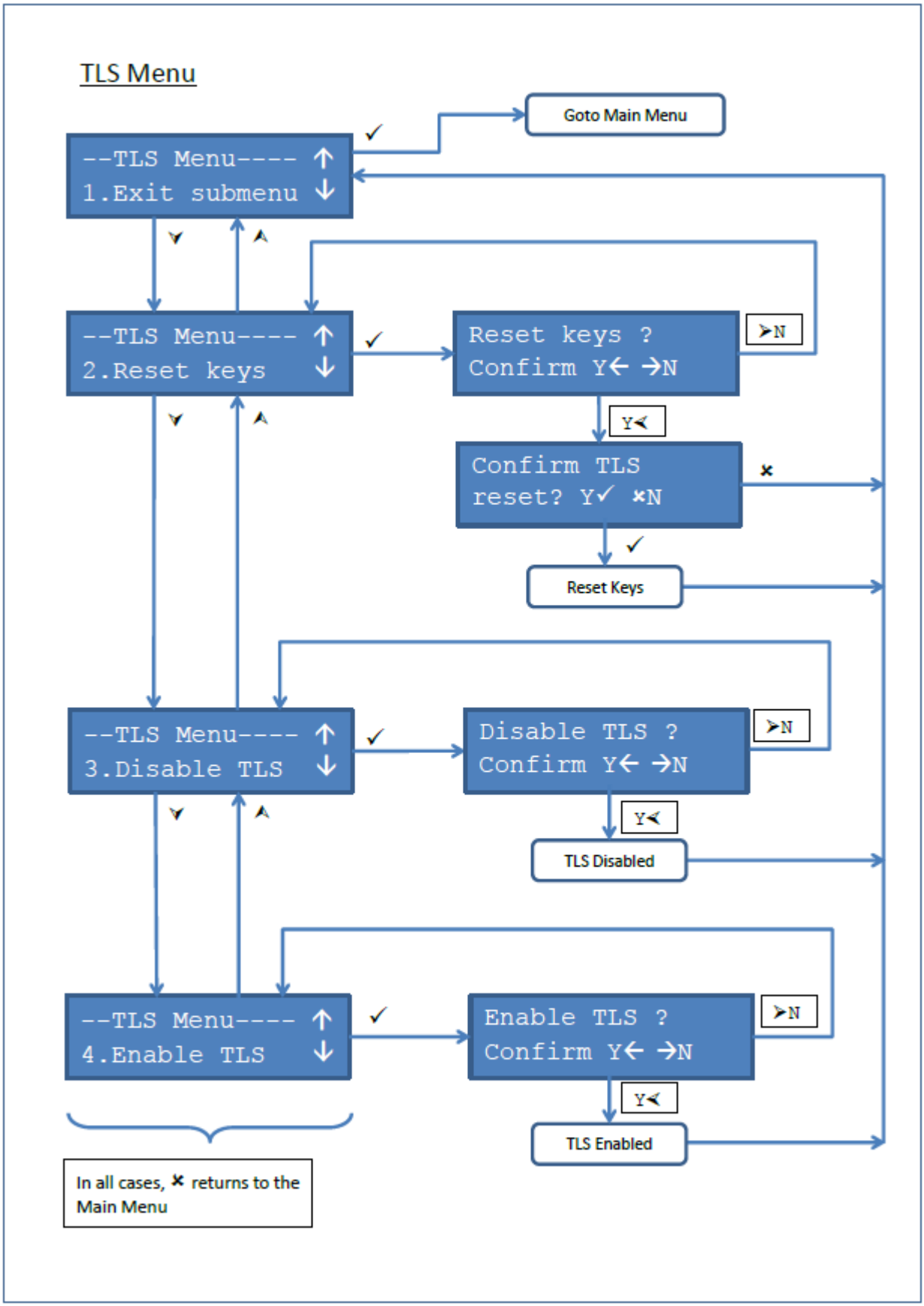
Refer to TSM500i-NSS SNMP Application Note (PR-D2-1121) for instructions on how to enable SNMP in TsmWeb.

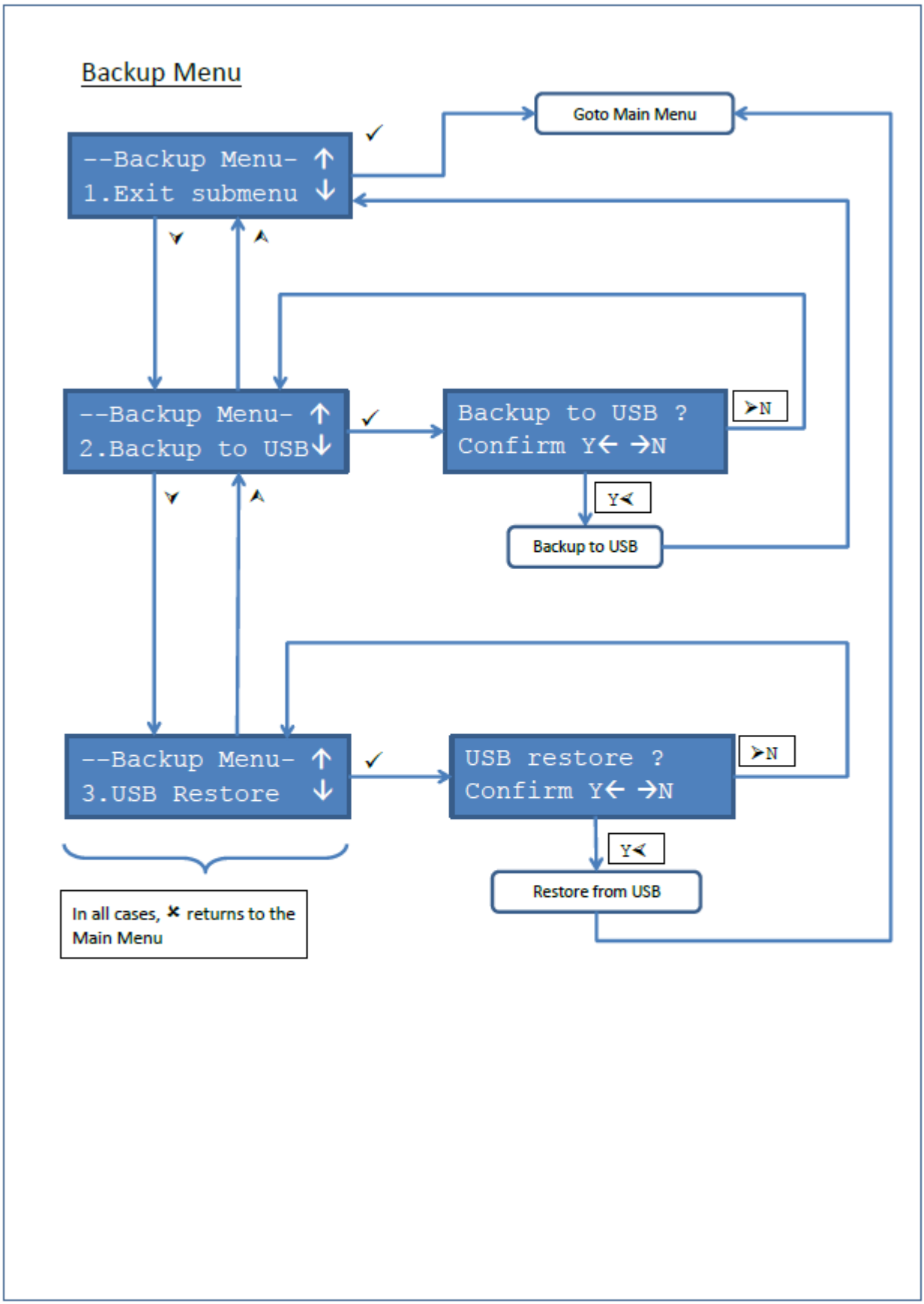
8.7 LCD Menu Sequence

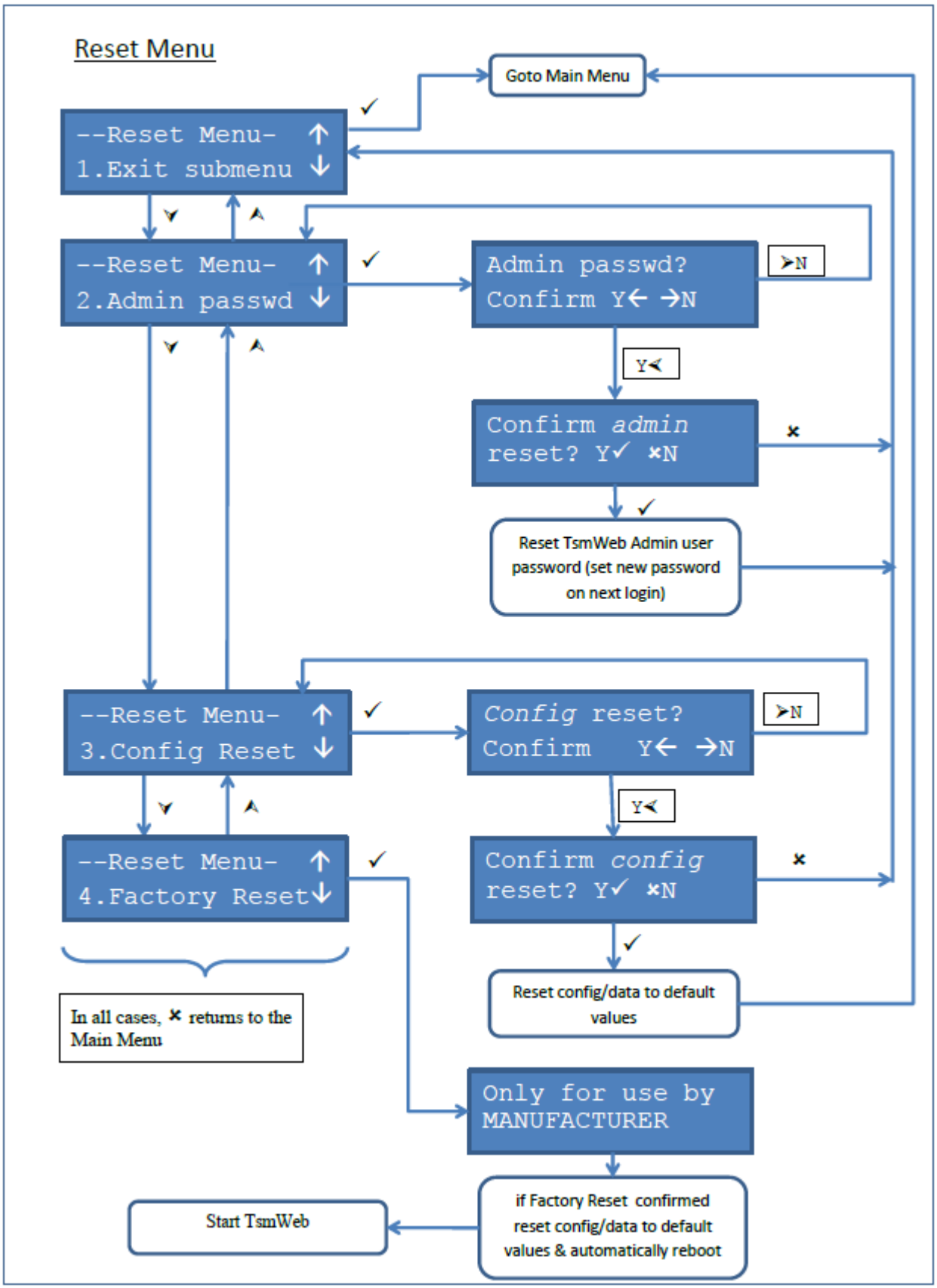



Main Menu
--Main Menu--
1.Exit & Boot
Start Webserver
--Main Menu--
2.TCP/IP...
Goto TCP/IP Menu
--Main Menu--
3.TLS settings
Goto TLS Menu
--Main Menu--
4.USB Backup...
Goto Backup Menu
--Main Menu--
5.Reset...
Goto Reset Menu
In all cases, * causes Main Menu to exit and webserver to start


TCP/IP Menu
Goto Main Menu
--TCP/IP Menu-
1.Exit submenu
--TCP/IP Menu-
2.IP Address
--TCP/IP Menu-
3.Netmask
--TCP/IP Menu-
4.Set Gateway
--TCP/IP Menu-
5.Clear Gateway
IP address*
Confirm Y← →N
Edit addr? Y← →N
192.168.000.201
Address (edit)
101.002.003.004
186.214.000.204
Save addr? Y← →N
Store change
Clear Gateway
Confirm Y← →N
Store change
In all cases, ✖ returns to the Main Menu
Address* is one of:
IP address, Netmask or gateway


TLS Menu
Goto Main Menu
--TLS Menu----
1.Exit submenu
--TLS Menu----
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

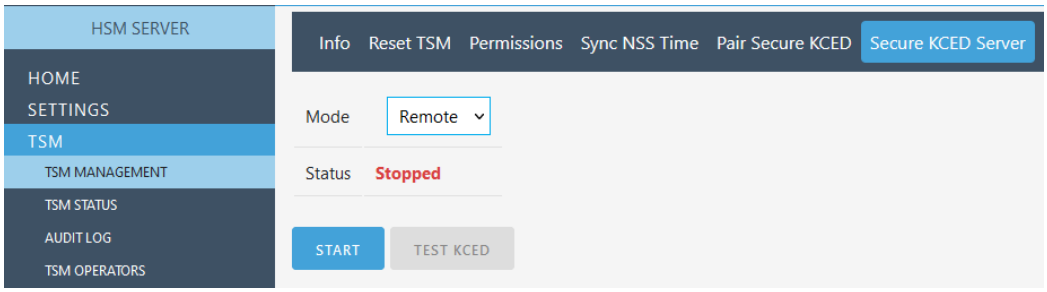

Reset Menu
Goto Main Menu
--Reset Menu-
1.Exit submenu
--Reset Menu-
2.Admin passwd
Admin passwd?
Confirm Y← →N
N
Y
Confirm admin
reset? Y✓ ×N
Reset TsmWeb Admin user password (set new password on next login)
--Reset Menu-
3.Config Reset
Config reset?
Confirm Y← →N
N
Y
--Reset Menu-
4.Factory Reset
Confirm config
reset? Y✓ ×N
Reset config/data to default values
In all cases, × returns to the Main Menu
Only for use by MANUFACTURER
if Factory Reset confirmed reset config/data to default values & automatically reboot
Start TsmWeb

9 Managing Your HSM

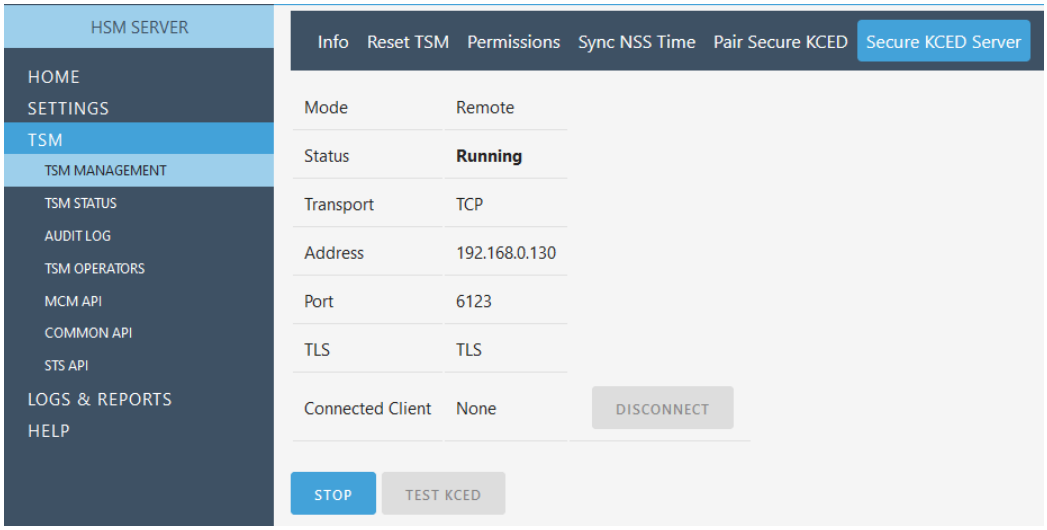
9.1 Managing the Secure KCED Service

The Secure KCED service works a little differently depending on the hardware version

For the TSM500i-NSS Hardware version:5520-00130_v1.1_NSS (stainless steel) this service is only applicable when using a the Secure KCED remotely. If the remotekced TsmWeb license has been loaded then remote use of the Secure KCED is supported. The state of the Secure KCED Service can be seen on the "Secure KCED Server" tab. If it is stopped then click the **Start** button

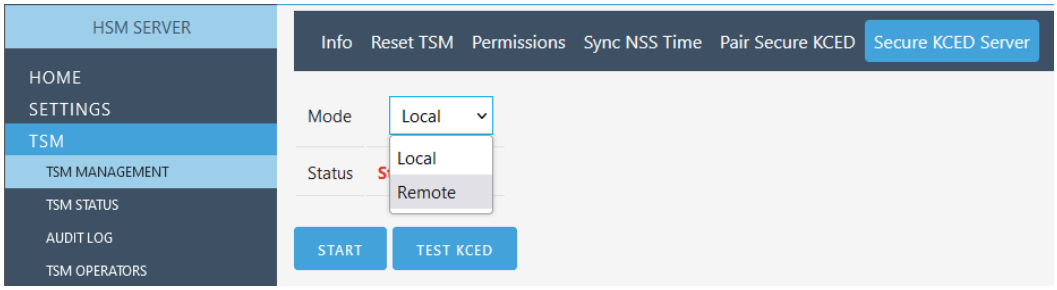


The screenshot below shows an example of the Secure KCED Service running normally in Remote mode



Refer to the Remote KCED User Guide (PR-D1-1113) for details on how to install, configure a Secure KCED for remote use.

TSM500i-NSS Hardware version:5520-00130_v1.2_NSS (Black case) this service supports local use of the Secure KCED by default. If the remotekced TsmWeb license has been loaded then remote use of the Secure KCED is also supported.



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.

9.2 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 section 4.1

9.3 HSM Password Management

9.3.1 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 2.8 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!**

9.3.2 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!**

9.3.3 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!**

9.3.4 Reset CSPs, Clear All Passwords, and Set Passwords

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 should NOT be used to set initial passwords - for that use 'Authenticate HSM & Set Initial Passwords' (see section 4.2).

This operation should only be used when ALL passwords have been forgotten.

This operation will result in the erasure of ALL CSPs and ALL passwords.

To proceed, the customer must send a signed letter to the Manufacturer requesting the reset certificate. The letter must include the names and email addresses of the two crypto officers that will set their passwords simultaneously and take control of the HSM after all secrets have been erased.

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
- Both Crypto Officers must have received their *Reset Password Token*, one for each Cryptographic Officer, sent individually to the email addresses specified on the signed letter. The tokens may only be **used once** where-after they will not function.
- Both Crypto Officers must be present during this command.

Process:

- Click on "Clear CSPs and Reset Passwords" tab on the ***TSM > TSM Operators*** page.
- Set "Officer 1 Name" and "Officer 2 Name" fields.
- Copy both tokens into their respective boxes and click on the **Clear CSPS and Reset Passwords** button.
- The first Crypto Officer must follow the instructions displayed on the **KCED.** There should be a message for Operator #1 to enter a new password. **The password must be entered via the KCED keypad**.
- A password must be at least 7 digits in length, using digits in the range 0 to 9.
- The KCED will prompt the first Crypto Officer to verify the password (enter it a second time).
- Once the password has been verified it is stored in the TSM500i.
- Make a record of the password and keep it locked in a safe when not in use.
- The second Crypto Officer (identified as Operator #2 by the TSM500i) will be prompted to set their password in the same way.
- **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!**

9.4 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.

9.5 Check Date & Time

Verify that the date & time of the TSM500i-NSS (reported at bottom of TsmWeb home page) and the time of the HSM are correct and synchronized. If not, setting the date and time in accordance with section 4.3 will set both clocks simultaneously.

9.6 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 be*BL: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.

9.7 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

9.8 Clear tamper

If the TSM500i is in a tampered state you will need to reset the tamper. This service requires two Crypto Officers to login to the TSM500i HSM using the KCED.

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

Before clearing the tamper, it is advisable to first ascertain the cause of the tamper. To do this, navigate to the ***TSM > TSM Status*** page and observe what is reported under the headings *Active Tamper* and *Latched Tamper*. If an **active** tamper is reported, then it means that the tamper condition is still present, and it will **not** be possible to clear this tamper. If a **latched** tamper is reported, then it means that the tamper condition was transitory and **can** be cleared. Make a note of the tamper type that is indicated.

Navigate to the ***TSM > TSM Management*** page, and select the "Tamper" tab. Click on the **Clear tamper** button to clear the tamper. Verify that the RED LED turns off.

10 Common Tasks for All Payment HSMs

10.1 Setting the TSM500i HSM's Operational Permissions

After setting the operational permissions the TSM500i must be returned to Operational state to prevent it from remaining in a Privileged state, which is a security risk.

The TSM500i firmware supports Access Control, allowing cryptographic officers to enhance system security by enabling or disabling certain functionality of the HSM.

Two cryptographic officers are required to authenticate themselves to the HSM in order to manage the Permissions settings.

- Navigate to the ***TSM > TSM Management*** page, and select the "Permissions" tab.
- A table should be shown which lists the state of each of the permissions as well as a recommended state.
- Note that this table represents the permissions that will be available to the HSM when in **AC:Operational** mode. Some permissions are only available in **AC:Privileged** mode, and will be dropped when returning to **AC:Operational** mode.
- To set permissions, edit the text box labelled "Permissions". This should be a list of permissions represented by respective mnemonics as shown in the permissions table.
- For each additional permission insert a space and then type in the mnemonic
- Once all required permissions have been entered, and those to be unset removed, click the **Set Permissions** button to apply the settings.

11 MCM (Payments) Tasks and User Interfaces

11.1 Generating SMK 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 SMK could be compromised.

Requirements:

- A KCED needs to be connected to the TSM500i-NSS.
- The TSM500i must be in the ***AC:Privileged*** mode.

To generate key components:

- Navigate to ***TSM > MCM API*** page and select the “Generate Key Components” tab.
- Select appropriate values of "Key Algorithm", “Key Size”, “Number of Components”, Verification Method” and “Parity” (for TDES keys) for the key.
- Click on the **Generate Components** button.
- The key components generated should be displayed on the KCED. Follow prompts on the KCED to ensure secrecy of the components.

The valid combinations of SMK type, size, and verification algorithm for Storage Master Keys are shown below:-

SMK Type	Size	Key Verification Method
TDES XOR	112 bits (double length)	DES/TDES KCV Algorithm
AES	128 bits / 192 bits / 256 bits	SHA256 hash over the value x’01 followed by the key.
AES-KB	128 bits / 192 bits /256 bits	CMAC KCV Algorithm

11.2 Loading SMK components

The TSM500i requires two Cryptographic Officers to authenticate themselves to the HSM to permit the loading of an SMK**.**

Key loading should take place according to established security procedures and is usually witnessed by an auditor.

Although the TSM500i HSM will revert to the Operational state after a period of time (as determined by the firmware license type and detailed in the Security Policy), the HSM should be set back to the **AC:Operational** mode after loading an SMK to prevent it from staying in a Privileged state once the Crypto Officers have completed this procedure.

The SMK must be generated and stored in the form of components, which are split between two or more trusted custodians. When the HSM is first commissioned (or after a Tamper event has been reset) the SMK must be loaded into the HSM using SMK components.

Key Spaces are used in some environments to establish key variants for exchanging keys between disparate systems. System documentation should indicate when special Key Space configurations are required.

All HSMs that use the same key database (i.e. HSMs in a load balancing or fault tolerant configuration) must have the same SMK and Key Space configuration.

Before proceeding, refer to the *KCED Installation and User Guide* for details on how to use the Key Component Entry Device (KCED).

Requirements:

- A KCED needs to be connected to the TSM500i-NSS.
- The TSM500i HSM must be in privileged state, i.e., the access control mode must be ***AC:Priviledged***, which requires that two Crypto Officers have authenticated with the HSM.

Procedure:

- A KCED will need to be connected to the KCED port on the front panel of the TSM500i-NSS.
- Navigate to ***TSM > MCM API*** page and select the “Load SMK” tab.
- Select algorithm type from the drop down menu labelled “Algorithm”. An AES-KB SMK is recommended
- Select appropriate values of "Key Algorithm", “Key Size”, “Number of Components” and “Verification Method”.
- To make the TSM500i forgo/skip checking the SMK key check value leave the “Key check Value” field blank. This is not recommended.
- Click on the **Load SMK** button.
- A confirmation page should be displayed. Read the warning, and if you wish to continue click on the **Yes, load SMK** button.
- Follow the on-screen instructions on the **KCED** display (NOT on TsmWeb) to enter the SMK.

11.3 Generating and Loading Operational Keys

If key components need to be generated for operational keys the system e.g. Base Derivation Key, PIN Verification Key and so on, then the same process as that used in section 11.1 can be used to generate components for each operational key.

The loading of operational key components is typically driven by the client software and the HSM needs to be in the ***AC:Privileged*** mode when the key components are entered using the KCED.

11.3.1 Loading a Key using TsmWeb

The TSM500i requires two Cryptographic Officers to authenticate themselves to the HSM to permit the loading of an SMK**.**

Key loading should take place according to established security procedures and is usually witnessed by an auditor.

Requirements:

- A KCED needs to be connected to the KCED port on the front panel of the TSM500i-NSS.
- The TSM500i HSM must be in privileged state, i.e., the access control mode must be ***AC:Priviledged***, which requires that two Crypto Officers have authenticated with the HSM.

To load a key:

- Navigate to ***TSM > MCM API***, and select the "Load Key" tab.
- Select appropriate values for "Key Token Format", "Key Type", "Number of Components", "Algorithm", "Key Size", "Key Parity", "Mode of Use", "Key Version Number", "Exportability" and "Key Check Value". Not all fields may be applicable, depending on the selected value of "Key Token Format". The check value is optional, but it is recommended that one is given.
- Click the **Load Key** button.
- Follow the on-screen instructions on the KCED display to enter the key components.

Note that TsmWeb displays the operational key encrypted under the SMK. It does not store this key, so it is the users responsibility to copy and save the operational key for future use.

11.4 Storage Master Key Migration

This functionality is NOT applicable on TSM500i HSMs with STS firmware.

The process of key migration (i.e. replacing an existing Storage Master Key (SMK) while maintaining all operational keys in the system) is NOT within the scope of this document. Contact Prism for assistance with key migration.

For details on how to load an SMK for the first time or to load a new SMK without maintaining operational keys, you should refer to Section 11.2.

11.4.1 Select SMK Migration tab and Login

A KCED will need to be connected to the KCED port on the front panel of the TSM500i-NSS.

To perform key migration, use a Web Browser to access TsmWeb (refer section 3.5). Expand "TSM" on the left hand menu. Select the "KEY MANAGEMENT".

If not already in the Privileged state, two Cryptographic Officers will be prompted to login in order to enter the ***AC:Privileged*** mode. The "TSM Key Management" page will reload after the cryptographic officers have successfully logged in to the TSM500i.

Click on "SMK Migration" tab on the "TSM Key Management" page.

11.4.2 Load a Migration SMK

Loading a migration SMK results in the active SMK being erased. This is a security measure to ensure that the custodians of the active SMK are present, and that SMK migration is done with their knowledge, because they must reload the active SMK after the Migration SMK has been loaded. The migration of operational keys can be done once when the TM500i has an Active SMK and a Migration SMK.

Key loading should take place according to established security procedures, and is usually witnessed by an auditor.

Before any key translation can be performed, a migration Storage Master Key (SMK) must to be loaded into the module.

- Click on **Load Migration SMK** if no migration SMK has been loaded
- Select algorithm type from the drop down menu labelled "Algorithm"
- Select key size from the drop down menu labelled "Key Size"
- Select the number of components from the drop down menu labelled "Number of Components"
- Select key check value algorithm from the drop down menu labelled "Verification Method"
- Enter key check value (optional).
- Click on **Load Migration SMK**
- A confirmation page should be displayed. To continue click on **Yes, load SMK**
- Follow the on-screen instructions on the KCED display to enter the SMK.

Proper measures must be taken to ensure that the component being entered is visible to nobody except the custodian responsible for the component otherwise the SMK could be compromised.

11.4.3 Set the Migration SMK as the Active SMK

- Click on **Set as Active**.
- A confirmation page should be displayed. To continue click on **Yes, activate SMK**

By performing this action, the active SMK will be replaced with the migration SMK, along with the associated key space.

11.4.4 Delete the Migration SMK

- Click on **Delete**.
- A confirmation page should be displayed. To continue click on **Yes, delete SMK**

12 Common API (Payments) Tasks and User Interfaces

12.1 Generating Key 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 key component could be compromised.

Requirements:

- A KCED needs to be connected to the TSM500i-NSS.

To generate key components:

- Navigate to ***TSM > Common API***, and select the "Generate Key Components" tab.
- Choose appropriate values for the "Key Algorithm" and "Number of Components" fields.
- Click the **Generate Components** button.
- The key components generated should be displayed on the KCED. Follow prompts on the KCED to ensure secrecy of the components.

12.2 Loading a Storage Master Key (SMK)

The TSM500i requires two Cryptographic Officers to authenticate themselves to the HSM to permit the loading of an SMK.

Key loading should take place according to established security procedures and is usually witnessed by an auditor.

Requirements:

- A KCED needs to be connected to the TSM500i-NSS.
- The TSM500i HSM must be in privileged state, i.e., the access control mode must be ***AC:Priviledged***, which requires that two Crypto Officers have authenticated with the HSM.

To load an SMK:

- Navigate to ***TSM > Common API***, and select the "Load SMK" tab.
- Select the Live "SMK Slot"
- Select appropriate values for "SMK Slot", "Algorithm", "Number of Components", "Parity" (for a TDES SMK), and "Check Value". The check value is optional, but it is recommended that one is given.
- If loading a migration SMK, confirm that the live SMK can be deleted.
- Click the **Load SMK** button.
- Follow the on-screen instructions on the KCED display to enter the SMK components.

12.3 Loading a Key block

The TSM500i requires two Cryptographic Officers to authenticate themselves to the HSM to permit the loading of a key.

Requirements:

- A KCED needs to be connected to the KCED port on the front panel of the TSM500i-NSS.
- The TSM500i HSM must be in privileged state, i.e., the access control mode must be ***AC:Priviledged***, which requires that two Crypto Officers have authenticated with the HSM.

To load a key block:

- Navigate to ***TSM > Common API***, and select the "Load Key Block" tab.
- Select appropriate values for "Key Algorithm", "Key Usage", "Key Size", "Number of Components", "Check Value", "Mode of Use", and "Exportability". The check value is optional, but it is recommended that one is given.
- Click the **Load Key Block** button.
- Follow the on-screen instructions on the KCED display to enter the key components.

12.4 Storage Master Key (SMK) Migration

12.4.1 How to Load a Migration SMK

The TSM500i requires two Cryptographic Officers to authenticate themselves to the HSM to permit the loading of an SMK.

Key loading should take place according to established security procedures and is usually witnessed by an auditor.

Loading a migration SMK results in the live SMK being deleted. This is a security measure to ensure that the custodians of the live SMK are present, and that SMK migration is done with their knowledge, because they must reload the active SMK after the Migration SMK has been loaded. The migration of operational keys can be done once when the TM500i has an live SMK and a migration SMK.

Requirements:

- A KCED needs to be connected to the TSM500i-NSS.
- The TSM500i HSM must be in privileged state, i.e., the access control mode must be ***AC:Priviledged***, which requires that two Crypto Officers have authenticated with the HSM.

To load an SMK:

- Navigate to ***TSM > Common API***, and select the "Load SMK" tab.
- Select the Migration "SMK Slot"
- Select appropriate values for "SMK Slot", "Algorithm", "Number of Components", "Parity" (for a TDES SMK), and "Check Value". The check value is optional, but it is recommended that one is given.
- If loading a migration SMK, confirm that the live SMK can be deleted.
- Click the **Load SMK** button.

- Follow the on-screen instructions on the KCED display to enter the SMK components.

12.4.2 Migrating a Key Block

If only a small number of keys need to be migrated, each key can be migrated manually using TsmWeb. If this is not practical, contact Prism for assistance in automating the migration process.

To migrate a single key block:

Requirements:

- Both live and migration SMKs need to have been loaded. Note that loading a migration SMK will erase the live SMK, therefore the live SMK needs to be reloaded after the migration SMK has been loaded.
- The “keymgmt” permission is required. See Section XX on how to set this.

Procedure:

- Navigate to ***TSM > Common API***, and select the “Migrate Key Block” tab.
- Fill in the “Key Block” field with the key block being migrated (encrypted under the live SMK).
- Click the **Migrate Key Block** button.

The migrated key block (encrypted under the migration SMK) will be displayed.

12.4.3 Setting the Migration SMK as the Live SMK

Once the key migration process has been completed, the migration SMK can be set as the live SMK. The live SMK will be overwritten by the migration SMK, and the migration SMK will be erased. To do this:

- Navigate to the ***TSM > Common API*** page, and select the “Dashboard” tab.
- In the “HSM Status” section, click the **TASKS** menu and the click “Activate Migration SMK” menu item.
- A warning message will appear. Make sure to read and understand the warning before proceeding.
- Click the **Activate Migration SMK** button.

13 Configuring & Testing Client Software

Client software must be configured to communicate with TSM500i HSM access service (Conductor service and/or Common API 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.

APPENDIX A – List of Abbreviations

BL	Boot Loader
CSP	Critical Security Parameter (for example, a password or a 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
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