TSM500i and TsmWeb User Guide

November 2019

Document number:	PR-D2-0854 Rev 2.9
Release date:	November 2019
Prepared by:	Giovanni Gallus
Copyright:	© 2019 Prism Payment Technologies (Pty) Ltd
Synopsis:	This document describes the TSM500 and TSM500i Hardware Security Modules (HSMs) as well as the TsmWeb interface used to manage this HSM.

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

www.prism.co.za

Document Structure

This document comprises the following sections:

⚠️ **Do NOT use the TSM500i without following all of the appropriate <u>security procedures</u> detailed in Section 0.**

⚠️ **The TSM500i HSM is shipped with <u>no passwords</u> for the Crypto Officer roles. The two crypto appointed officers must <u>set their passwords</u> in accordance with section 2.8. This step is also used to authenticate the origin of the HSM.**

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

Section 1: TSM500 Overview

This section contains information that describes your TSM500i Hardware Security Module (HSM), its interfaces and its status indicators. It is very important to read this section before proceeding with installation and operation of your TSM500i HSM. This document also applies to the previous HSM model, the TSM500, so where it refers to the TSM500i it also applies to the TSM500.

Section 2 : Installation and Security Procedures

This section outlines the correct handling and installation of a TSM500i. It also describes the setup and <u>security procedures</u> that must be followed when commissioning an HSM.

Follow all the steps provided in Section 2 to get your new TSM500i operational.

Section 3 : Ongoing maintenance

This section provides details on how to use and manage your TSM500i after initial deployment. In includes information on additional settings and services available through TSM-WEB and the NSS Boot Menu.

Section 4 : STS

This section contains information that is ONLY relevant to a TSM500i HSM with STS firmware. Sections 1 to 3 also apply to HSMs with STS firmware except where specifically noted otherwise.

Contents

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

www.prism.co.za

1 TSM500i 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 also applies to the previous HSM model, the TSM500, so where it refers to the TSM500i it also applies to the TSM500.

1.1 TSM500i-PCIe DESCRIPTION

The TSM500i-PCIe is a Hardware Security Module (HSM) with a PCI Express interface. It also includes a serial interface for loading Critical Security Parameters (CSPs).

When using a TSM500i-PCIe, it is the user's responsibility to procure and setup a server that will house the TSM500i-PCIe. Note that a physical computer is required – the TSM500i-PCIe cannot be installed in a virtual machine. It is also necessary to install drivers and other support software such as Conductor, TSM-WEB and the Java 2 Runtime Environment.

1.2 TSM500i-NSS DESCRIPTION

The TSM500i-NSS is a network appliance that includes a TSM500i-PCI packaged together with an embedded computer system. This solution has an Ethernet interface and also includes a serial interface for loading CSPs. A 2-line 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 **TSM-WEB** application and supporting drivers. This configuration is easier to manage than the TSM500i-PCIe. Below is a simplified view of what is inside the TSM500i-NSS and how it inter-connects.
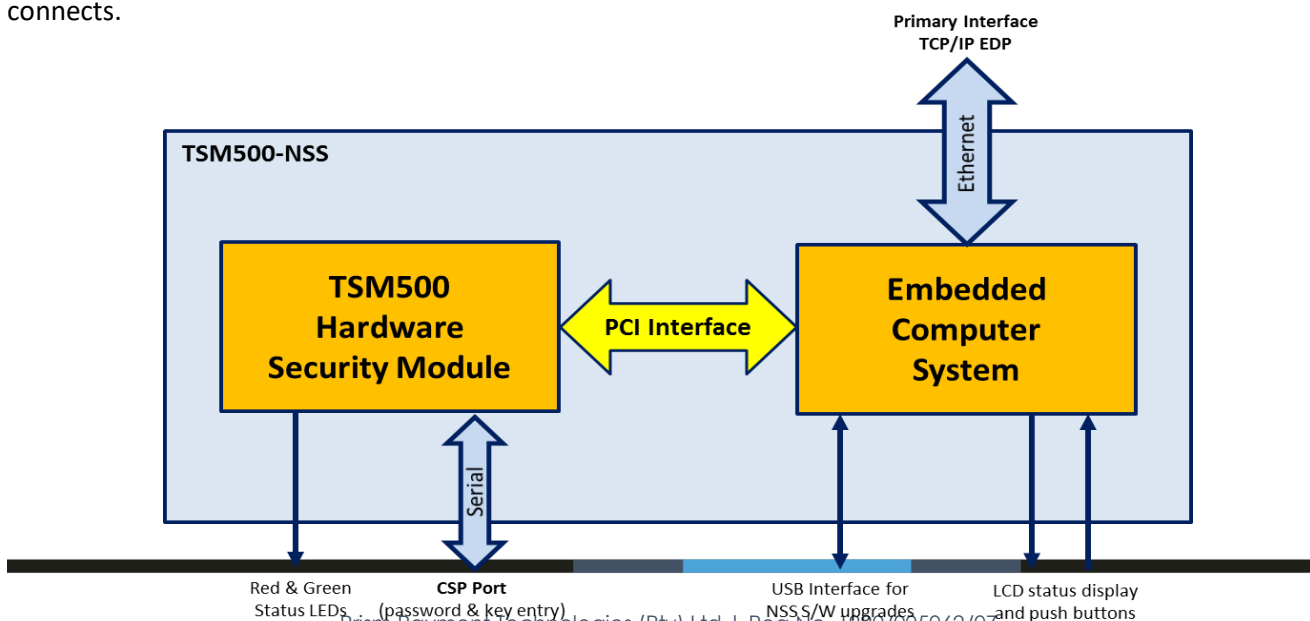
1.3 KCED DESCRIPTION

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

- Entry of Cryptographic Passwords (refer section 2.8)
- Entry of Key Components (refer section 2.12)
- Generation of Key Components (refer section 2.12)

The KCED connects directly to the TSM500i hardware security module by means of a serial interface. In the case of a TSM500i-NSS, it connects to the "KCED" port on the front panel. In the case of a TSM500i-PCIe, it connects to the RED port on the connector panel (this is the connector closest to the status LEDs).

TSM500i-PCIe KCED PORT

TSM500i LEDs

TSM500i LEDs   **TSM500i-NSS KCED PORT**
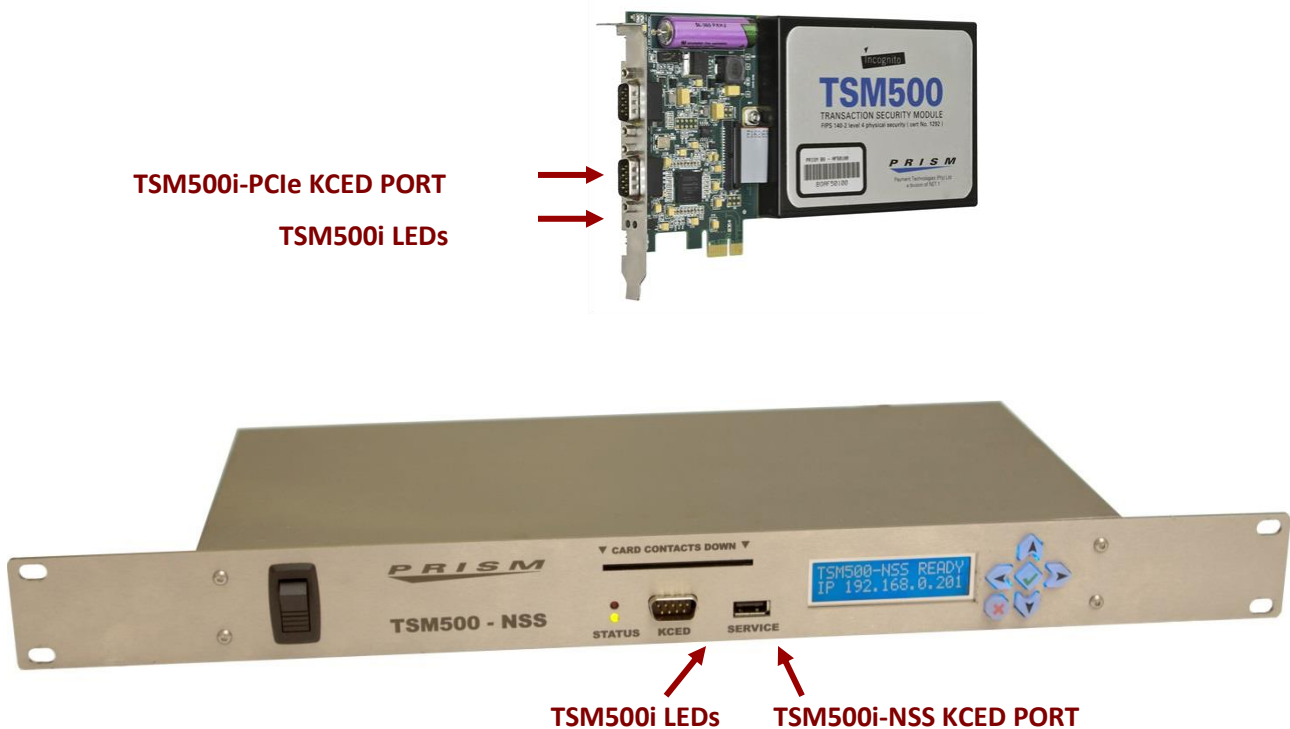
The above photographs identify the 9-way connector to be used by the KCED on the TSM500i-PCIe and TSM500i-NSS.

For detailed information on how to install and use the KCED, refer to the following guide that may be found on the TSM5XX Support CD:

   KCED Installation and User Guide.pdf

2 INSTALLATION & SECURITY PROCEDURES

2.1 QUICK GUIDE: FROM INSTALLATION TO OPERATION

(See 2.2)

Establish Security Procedures

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**

(See 2.3)

Inspect and Install Hardware

The TSM500i NSS / PCIe hardware must be inspected and then installed in a secure environment in accordance with the procedures detailed in this user guide

(See 2.4)

Check Physical Indicators

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

(See 2.5)

PCIe: Install Driver & SW

PCIe ONLY: Install device driver. Run TSM500 PCI Installer which installs Conductor, documentation & TSM-WEB. Install Java J2RE.

(See 2.6)

NSS: Network Setup

NSS ONLY: Set the IP address and network mask (netmask) using the Boot Menu which is accessed via the front panel

(See 2.7)

Access TSM-WEB Interface

Enter the IP address into a Web Browser on a PC that is connected to the same subnet to access TSM-WEB. Set the TSM-WEB admin user account password. Login to TSM-WEB as admin and perform a basic functionality test.

(See 2.8)

**Set TSM500 Passwords;
(Clear Tamper);
(Set Date & Time)**

The TSM500i is shipped **without Crypto Officer passwords**. *Officers must be assigned to the TSM500i according to the security procedures, and must set their passwords using password reset tokens supplied by Prism.*
In the rare case that shipping triggers a Tamper event, it will be necessary to clear/reset this condition. If required, the date and time can be set to match your time zone

(See 2.9)

Configure and Test Conductor

TSM500i-NSS: Conductor is preinstalled and is managed by TSM-WEB.
TSM500i-PCIe: Use Conductor Setup to configure and install a Conductor service. See Conductor User Guide for more details.

(See 2.10)

TSM-WEB Access Control

Setup TSM-WEB access control by creating TSM-WEB user accounts, setting the password policy and default auto-logoff times

(See 2.11)

Backup Settings

Follow the backup procedure to backup TSM-WEB settings:

(See 2.12)

Prepare TSM500 for Operation: Load CSPs

CSPs must be loaded into the TSM500i 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.

(See 2.13)

Configure and Test Client Software

Client software must be configured to communicate with Conductor and/or the TSM500i, then tested to ensure that transaction processing can proceed successfully. Third-party tools will be used during this step.

2.2 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.

2.3   INSPECT AND INSTALL HARDWARE

2.3.1   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 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.

- Request for Password Reset Certificates from Prism. Refer to Notice – TSM5XX Password Reset Certificates on the TSM5XX Support CD.

  Each crypto officer will receive their password reset certificates from Prism that is used to authenticate Prism as the manufacturer and then allows the crypto officer to set their password.

⚠️ **Contact Prism immediately if the serial tamper evident stickers have been interfered with or if the hardware is in the tampered state.**

2.3.2   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".

2.3.3   TSM500i-PCIe Hardware Installation

The following steps are to be followed when installing the TSM500i-PCIe into a PC. The term PC here also applies to servers.

- Locate the PC's card installation documentation and ensure that you are familiar with the safety instructions and precautions conveyed in this document.

- Turn OFF the PC and ensure all attached devices are also off.

- Remove the cover from the PC and locate a suitable PCI express expansion slot (as described in Section 1). Access to the expansion slot may differ for machines from different vendors, please refer to your vendor documentation.

- Remove the TSM500i from the protective static bag.

⚠️ **To prevent Electro Static Discharge, it is advisable to wear an anti-static wrist strap when handling the card. Failure to do so may result in the module entering the Tampered State.**

The following precautions <u>MUST</u> be used when not using an anti-static wrist strap.

o Ground yourself by making contact with the case of the machine for at least 2 seconds.

o Limit your movements as to prevent excessive build-up of static electricity.

o Handle the card at its edges only. Do not touch exposed circuitry and components.

- Insert the module into an available PCI express slot ensuring that the card is correctly seated.

- Secure the card to the case using the appropriate screws.

- Replace all covers and reattach all cables that were disconnected.

2.4 CHECK PHYSICAL INDICATORS (LEDs)

After powering on the TSM500i-NSS or the PC in which the TSM500i-PCIe is installed.

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

- For the TSM500i-NSS, the status LEDs are located on the front panel
- For the TSM500i-PCIe, the status LEDs are located on the connector panel.

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)

2.5 INSTALL DRIVERS, CONDUCTOR & TSM-WEB

This section only applicable to the <u>TSM500i-PCIe</u> (it does not apply to a TSM500i-NSS).

For a TSM500i-PCIe, perform the following steps:

- **Install the Driver**

  Refer to the readme.txt file provided in the Driver folder of the TSM5XX Support CD to select the appropriate driver for your Windows operating system.

- **Install Conductor and TSM-WEB**

  Run *TSM5XX-PCI_Installer.exe* (provided on the TSM5XX Support CD). This will install the Conductor service and TSM-WEB.

- **Install Java Runtime Environment (JRE)**

  JRE v1.4.2 is provided on the TSM5XX Support CD. This is the recommended version that should be installed before attempting to use Conductor.

- **Setup Conductor**

  Run *ConductorSetup.exe*. Refer to the *Conductor User Guide* for details on how to setup Conductor. This may be found in *Start -> Prism -> Conductor* after installing Conductor and is also on the TSM5XX Support CD.

2.6   NETWORK SETUP & RECOVERY

This section only applicable to the <u>TSM500i-NSS</u> (it does not apply to a TSM500i-PCIe).

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 *BOOT MENU* (see section 2.6.1). The alternative is to access the NSS using the default address and change it later using the TSM-WEB interface.

It is also possible to use the boot menu to reset the configuration to its defaults, reset the NSS to factory state and to reset the TSM-WEB admin password.

2.6.1   Use the BOOT MENU to set the IP address

To access the BOOT 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 BOOT 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 BOOT MENU appears.

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

BOOT MENU

1.   Continue boot
2.   IP Address
3.   Netmask
4.   Backup to USB
5.   USB Restore
6.   Disable TLS
7.   Reset…

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

Use the arrow keys and green accept key to select the **IP Address** option. This will allow the setting of the IP address. The menu option **Netmask** may be used to set the required netmask.

To change an address (either the IP address or netmask), 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 BOOT MENU can be found in <u>APPENDIX A – LCD SEQUENCE</u>.

2.7 ACCESS TSM-WEB INTERFACE

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

2.7.1 Invoking TSM-WEB for a TSM500i-PCIe

Enter http://localhost as the URL into your Web Browser when using TSM500i-PCIe.

Note that TSM-WEB and Conductor must have been installed (see section 2.5).

2.7.2 Invoking TSM-WEB 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://196.214.189.219 on a PC that is connected to the same subnet to access TSM-WEB. 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).

2.7.3   Setting the TSM-WEB admin password

⚠️ *User / Password Setup is not applicable to a TSM500i-PCIe when using TSM-WEB from the computer that hosts the TSM500i-PCIe when you click* `Login as $Local`*. When accessing it remotely it behaves the same as the TSM500i-NSS which means TSM-WEB user accounts will be required.*

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

⚠️ The TSM-WEB 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 TSM-WEB with a TSM500i-NSS, it is necessary to LOG IN to TSM-WEB in order to access any of the menus other than the *Home* page. The web browser will be re-directed to the SSL-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".

2.7.3.1   Setting Admin Password for the first time

If no admin user password has been set, the user will be presented with a screen titled ***TSM-WEB 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 and then click `Set Admin Password`.

Once a password has been entered for the *admin* user, the ***TSM-WEB 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 6 characters and must include at least one of each of the following:

- Upper case character
- Lower case character
- Digit

2.7.3.2   Resetting Admin Password

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 BOOT 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 BOOT MENU and then press the green accept key to continue booting.

Once the TSM500i-NSS has powered up, a new admin password for TSM-WEB may be set in accordance with section 2.7.3.1.

2.7.4   Using TSM-WEB for the first time

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

Click *TSM* from the side menu, wait for the *TSM management* page to load, then click on TSM Status Report which will retrieve a detailed status report from the TSM500i. Read the report to identify any problems.

If the Access control mode is **BL:TAMPERED_ROLE_NONE** then it means that the TSM500i is in the tampered state. To resolve this problem, refer to section 2.8.

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 Prism.

⚠️ **TSM-WEB will automatically log the user off after a default of 10 minutes of inactivity.**

ⓘ When using TSM-WEB on a TSM500i-NSS, you will always be required to enter a password. When using a TSM500i-PCIe, a password is not required when using TSM-WEB on the host computer, but is required if TSM-WEB is accessed from a remote computer.

Refer to sections 2.7.3 and 2.10 for details on how to setup a TSM-WEB admin password and further user passwords.

2.7.5   Accessing TSM-WEB through a different subnet

In some instances it may be necessary to access TSM-WEB 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 TSM-WEB through the firewall.

When your client computer is on a different subnet to the TSM500i-NSS needs 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.

Click *Network Settings* from the side menu, wait for the *Network settings* page to load, edit set the default gateway to the IP address of the default gateway, where your TSM500i-NSS is installed, and click Change settings .

2.8 SET TSM500i PASSWORDS, (CLEAR TAMPER) AND SET DATE & TIME

⚠️ **The TSM500i HSM is shipped without any Cryptographic Officer passwords for its administrative functions. The passwords for the two appointed Cryptographic Officers must be set immediately by using the *Reset Password Certificates* supplied by Prism. This operation also serves to authenticate the origin of the HSM.**

⚠️ The cryptographic officer passwords reside inside the HSM. They must not be confused with, and are not related to, the TSM-WEB user account passwords.

Requirements: Logged into TSM-WEB and the KCED connected to the TSM500i.

2.8.1 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* or *Loader Tampered* 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 (i.e. none, crypto-officer or crypto-user)

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_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: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 to Loader** in the *TSM management* page. 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.

2.8.2   Set the TSM500i Crypto Officer Passwords

To set the passwords, first put the TSM500i module into the *Loader or Loader Tampered* **state**. No authorised role needs to have been assumed.

i.e. *Access Control Mode* should be   BL:LOADER_ROLE_NONE   *or*
                                             BL:TAMPERED_ROLE_NONE

Prism will supply two *Reset Password Tokens* – one for each Cryptographic Officer. via e-mail. These tokens may only be **used once** where-after they will not function. When receiving tokens for two operators (i.e. two Cryptographic Officers), **always use the token for Operator #1 before using the token for Operator #2**. Failure to do so will result in the token for Operator #1 not working and another token will need to be issued by the manufacturer.

Click **TSM** from the side menu and wait for the *TSM management* page to load. Scroll down until you see the Reset Password button. The following procedure to set Operator #1 password:

1. Copy the first Password Reset token into the box and click on Reset Password which will allow the Operator #1 (the first Crypto Officer) to set a password.

2. The first Crypto Officer must look at the **KCED screen** that should show 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.

3. The KCED will prompt the first Crypto Officer to verify the password.

4. Once the password has been verified it is stored in the TSM500i.

5. **Make a record of the password and keep it locked in a safe when not in use**. The password will be required later in the setup procedure when loading key components.

The second Crypto Officer (identified as Operator #2 by the TSM500i) can set their password in the same way using the second password token.

⚠️ The Cryptographic Officers will be required to enter their passwords on the KCED at a later stage in order to load CSPs into the TSM500i.

2.8.3   [Optional Step] Clear Tamper

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

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

To login, specify the appropriate *Operator ID* and click Login (from the *TSM management* page). Before clearing the tamper, it is advisable to first ascertain the cause of the tamper. To do this, click on TSM Status Report (within the *TSM management* 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.

Click on Clear tamper to clear the tamper. Verify that the RED LED turns off.

2.8.4   [Optional Step] Set Date and Time

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.

In the browser on the *TSM management* page scroll down until you see Set date and time section. 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.

2.8.5   Put the TSM500i back into the Application 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 to App** from the *TSM management* page. Allow about 20 seconds (until green LED is flashing) for the TSM500i module to complete its initialisation before attempting to communicate with it again.

2.9   CONFIGURING AND TESTING CONDUCTOR

2.9.1   Configuring Conductor on the TSM500i-NSS

It is not necessary to configure and test Conductor on the TSM500i-NSS. The default settings will work in most environments. TSM-WEB allows the user to manage the Conductor port, the trace level and/or the maximum number of socket connections via the *Conductor Settings* menu.

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

2.9.1.1   *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.

2.9.1.2   *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.

2.9.1.3   *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.

2.9.1.4   *Restarting Conductor*

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

2.9.2   Configuring Conductor on the TSM500i-PCIe

When using a TSM500i-PCIe in a server where Conductor and TSM-WEB have been installed Conductor is managed using Conductor Setup. Refer to the *Conductor User Guide* (PR-D2-0535) which was installed with Conductor (see Start -> Prism -> Conductor) and is also available on the TSM5xx Support CD.

2.10 SETUP TSM-WEB ACCESS CONTROL

When using a TSM500i-NSS in an EFT payment system or key injection solution for terminals, TSM-WEB 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.

2.10.1 Create users

Each TSM-WEB user account should uniquely identify one user. No account should be usable by more than one individual.

To create a new user account click **Users** from the side menu and wait for the *Users* page to load, then click on the New User link. Enter all the new user's particulars and get them to enter their password and confirm it.

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 CCYY-MM-DD.

Once the user account expires the user will no longer be able to login to TSM-WEB.

2.10.2 Configuring Account and Password Policy

TSM-WEB account and password policy is configured in the *Preference Manager* which is accessed by clicking **Preference Manager** from the side menu. 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 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 Set .

2.10.3 Change Auto-Logoff Timeouts

Session/Auto-logoff timeouts are configured in the *Preferences Manager* which is accessed by clicking **Preference Manager** from the side menu.

The scroll down the list of preferences until you the following:

- session.timeout.absolute
- session.timeout.idle

2.10.4 Disable the default admin account

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

To do this, a user other than the default *admin* user and with an account that has the admin role, must login. They must then change the role of the *admin* user to 'none'.

2.11 BACKUP NSS SETTINGS

The TSM500i-NSS supports a backup of NSS data store (which includes network settings, conductor settings, user configuration and preferences) and log files to USB flash drive using the LCD BOOT MENU.

- Power the TSM500i-NSS off.

- Insert a USB flash drive 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 a BOOT MENU appears on the LCD display. Refer to APPENDIX A – LCD SEQUENCE for a flow chart of the Boot menu functions.

- Scroll down to Backup to USB option on the boot 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.

2.12 PREPARE TSM FOR OPERATION: LOAD CSPs

This section covers operational preparation for all TSM500i HSMs <u>except</u> those that are running STS firmware.

The most important CSP in a HSM is usually the **Storage Master Key** (**SMK**). This key is used to encrypt all other keys which are stored in a key database (outside the HSM). Without the SMK, the HSM is unable to perform any processing.

2.12.1 Generating SMK components

This service is only available then the TSM500i is in the *Privileged* mode.

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

- To perform SMK loading, use a Web Browser to access TSM-WEB (refer section 2.7). 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 "Generate Key Components" tab on the "TSM Key Management" page.

- The valid combinations of SMK type, size, and verification algorithm for **<u>Storage Master Keys</u>** 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

- Select algorithm type from the drop down menu labelled "Key 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".

- Select the required parity from the drop down menu labelled "Parity".

- Click on **Generate Components** .

- The key components generated should be displayed on the KCED. Follow prompts on the KCED to ensure secrecy of the 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.

2.12.2 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.

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.

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).

Procedure:

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

- To perform SMK loading, use a Web Browser to access TSM-WEB (refer section 2.7). 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 "Load SMK" tab on the "TSM Key Management" page.

- 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 SMK** .

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

- Follow the on-screen instructions on the **KCED** display (NOT on TSM-WEB) to enter the SMK.

⚠️ TSM500 HSMs with versions of Application Firmware prior to v3.0.0 should be set back to the **AC:Operational** mode after loading an SMK or else the TSM500 will remain in a Privileged state, which is a security risk. This does not apply to the TSM500i as its Application firmware starts from v3.0.0.

2.12.3   [Optional] Setting the TSM500i HSM's Operational Permissions

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 Access Control settings.

- Two cryptographic officers must login using the KCED in order to enter the **AC:Privileged** mode.

- On the TSM page, locate the table that shows each of the permissions available. The table 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 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.

- Once all of the required permissions have been entered, and those to be unset removed, click on **Set permissions** to apply the settings.

⚠️ The TSM500i must be returned to Operational state to prevent it from remaining in a Privileged state, which is a security risk**.**

2.13 CONFIGURING & TESTING CLIENT SOFTWARE

Client software must be configured to communicate with Conductor and/or the TSM500i, 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.

2.13.1   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 2.12.1 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.

3 ONGOING MAINTENANCE

3.1 Check Operational vs Privileged state

⚠️ *This paragraph is not applicable to TSM500i HSMs that are running STS firmware.*

Verify that the TSM500i is in the Operational state and that it has not accidentally been left in the Privileged state.

For HSMs with firmware versions of 3.0.0 or later, this step is not necessary since such HSMs will auto-logoff from the Privileged state after a pre-defined period of time. The time period is dependent on the type of firmware, but never exceeds 12 hours.

3.2 Check Date & Time

Verify that the date & time of the TSM500i-NSS (reported at bottom of TSM-WEB home page) and the time of the HSM are correct and synchronized. If not, setting the date and time in accordance with section 2.8.4 with set both clocks simultaneously.

3.3 Preference Manager

Click **Preference Manager** from the side menu to load the *Preference Manager* page which 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 TSM-WEB settings and are not stored on the HSM. When a backup to USB, see section is done all the preferences are included in the backup.

3.4 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 2.12.2.

3.4.1 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 TSM-WEB (refer section 2.7). 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.

3.4.2 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.

3.4.3 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.

3.4.4 Delete the Migration SMK

- Click on **Delete**.

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

3.5   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.

Click on TSM Status Report 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 the last 100 module Bootloader Audit Log entries (or less if the total logs to date is less than 100). 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 Application Log containing the last 100 module Application Audit Log entries (or less if the total logs to date is less than 100).

3.6   NSS Log Files

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

- TSM500i-NSS boot logs
- Conductor logs
- TSM-WEB start-up log

In addition to these log files TSM-WEB also logs all web browser interaction from users in its database. This activity can be viewed using various Reports which can be accessed via the *Reports* page from the side menu.

3.7   NSS Boot Menu

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

The TSM-WEB Boot Menu many 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 BOOT 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 BOOT MENU, refer to section 2.6.1 or APPENDIX A – LCD 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 1.2 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 2.7.3.2
- Set IP Address & Netmask   - refer to section 2.6.1
- USB Backup & Restore   - refer to section 0
- Reset to Defaults   - refer to section 3.9
- Disable SSL/TLS   - refer to section 3.11

3.8 Backup and Restore

3.8.1 Backup & Restore on a TSM500i-NSS

⚠️ *This procedure is only applicable to the **TSM500i-NSS** (it does not apply to a TSM500i-PCIe).*

Backup

Refer to section 2.11 for the procedure to backup NSS settings and the TSM-WEB 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.

- 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 a BOOT MENU appears on the LCD display. Refer to APPENDIX A – LCD SEQUENCE for a flow chart of the Boot menu functions. This takes approximately 20 seconds.

- Scroll down to USB Restore option on the boot 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 boot menu to appear. Select Continue Reboot.

3.8.2   Backup & Restore on a TSM500i-PCIe

*This procedure is only applicable to the **TSM500i-PCIe** (it does not apply to a TSM500i-NSS)*

Backup/restore functionality can be implemented via 3rd party software, which is not provided with the TSM-WEB software. The *sqlite3.exe* application that is required for live backup can be obtained from http://www.sqlite.org.

Offline backup
- This requires the "Prism TSM-WEB" service to be stopped and then restarted once the backup is complete.
- Backup the files tsmweb.sqlite and tsmweb.prop found in C:\Program Files\Prism\TsmWeb using a file backup program (e.g. NtBackup).

Live backup
- This backup can be done safely using a file backup program while TSM-WEB continues to run.
- To back up tsmweb.sqlite while TSM-WEB is running, we recommend using the sqlite3.exe application. Example of use:

    echo .backup tsmweb-snapshot.sqlite | sqlite3.exe "c:\Program Files\Prism\TsmWeb\tsmweb.sqlite"

- Backup tsmweb.prop found in C:\Program Files\Prism\TsmWeb using a file backup program (e.g. NtBackup).

Restore
- This requires the "Prism TSM-WEB" service to be stopped and then restarted once the restore is complete.
- To restore, simply copy the backup files to the original source location.

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

www.prism.co.za

3.9   Reset NSS to Default Settings

Section 3.7 details how to access the Reset submenu from the NSS Boot Menu. The Reset Menu includes a number of options and the associated default values are detailed below:

3.9.1   IP Addr Reset

Selecting the "IP addr reset" option from the *RESET MENU* will reset the IP address to the factory default value of 192.168.0.201.

3.9.2   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")

3.9.3   Factory Reset

Selecting the "Factory Reset" option from the *RESET MENU* will result in everything that is reset by the "Config Reset" option in addition to deleting all database files including the logs.

ⓘ   *It should never be necessary to reset to factory default settings during the normal life cycle of a TSM500i-NSS – please consult Prism support before resetting to factory defaults.*

3.10 SSL/TLS Certificate

SSL / TLS support was added to TSM-WEB from v3.21.0 onwards. When logging into TSM-WEB, the web browser will be re-directed to the SSL-secured log-in page.

When TSM-WEB generates a certificate, it assigns it a validity period of 2 years. The TSM Page displays the TLS certificate expiry date.

The TSM-WEB 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 TSM-WEB.

Steps to Generate a New TLS Certificate:

A new certificate can be generated via the "System" page within TSM-WEB. There are two options available:

- Click **Regenerate Certificate** to simply regenerate the server certificate used for TLS connections.

- Click **Regenerate Key & Certificate** to generate a new key-pair and certificate for the web server to use in TLS connections.

The TLS key algorithm can be changed via the "Preferences Manager", both RSA and EC key types are supported. It must be noted however that EC is not supported in Internet Explorer but has been tested successfully in both Mozilla Firefox and Google Chrome.

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. Therefore, if a user is unable to connect to the web server, on a secure connection, due to its certificate having expired, the TSM-WEB server needs to be restarted. The TSM500i-NSS will need to be rebooted for this to happen.

3.11 Disabling and Enabling SSL / TLS

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

3.11.1 Disable TLS from the BOOT MENU

Using the BOOT MENU as described in section 3.7, select the "Disable TLS" option and confirm the operation. The TLS service is now disabled.

3.11.2 Disable or Enable TLS from TSM-WEB

TLS cannot be re-enabled via the BOOT MENU. To enable or disable TLS via TSM-WEB, select "Preference Manager" from the side menu. Edit the *tls.enabled* preference as required.

After enabling TLS from TSM-WEB, it will be necessary to power-cycle the TSM500i-NSS in order to start the TLS service.

3.12 Upgrading TSM500i firmware

A TSM500i ships from Prism with the customer-specified version of firmware. If you receive an upgrade from Prism, login to TSM-WEB and select *TSM* from the side menu to load the *TSM management* page. Click on Reset to Loader in the *TSM management* page to set the TSM500i HSM to the ***Loader*** state. Additionally, if the firmware to be loaded is of a different type OR if the firmware version is earlier than the current version, then the Crypto Officer role will need to be assumed.

When updating the TSM500i firmware, the *Access Control Mode* should be:

> *BL:LOADER_ROLE_**NONE*** if loading firmware of same type & later version

> *BL:LOADER_ROLE_**OFFICER*** if loading firmware of different type or earlier version

Scroll down to the Update TSM firmware section of the *TSM management* page, browse to the file that was provided by Prism and then click on Update Firmware . To launch the application after the firmware has been successfully loaded, click on Reset to App .

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

A firmware <u>upgrade</u> 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.*

3.13 Upgrading TSM500i-NSS System Software

⚠️ *This section is only applicable to the **TSM500i-NSS** (it does not apply to the TSM500i-PCIe).*

ⓘ **Upgrading the TSM500i-NSS System Software 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 1.2). The embedded computer system has its own operating system and, amongst other things, runs the Conductor service and provides the TSM-WEB 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:

- Copy the upgrade files the NSS_UPDATES directory to the root path of a USB flash disk

- Power the TSM500i-NSS **off**

- Insert the USB flash disk 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.

3.14 Change Crypto Officer Password

This section is only applicable to <u>changing</u> an HSM Crypto Officer password when the current password for that Crypto Officer is <u>known</u>. In the event that the current password has been lost or if a password has never been set since taking delivery, a new password certificate must be issued by Prism. Thereafter, you will need to follow the steps detailed in section 2.8.2.

- Operator 1 = Crypto Officer #1

- Operator 2 = Crypto Officer #2

To change an existing password, first set the TSM500i module to the *Loader* state.

Only the currently logged in operator can change their password.

To change a password, first login by specifying the appropriate *Operator ID* and then click on <kbd>Login</kbd> (from the TSM menu).

Once logged in, click on <kbd>Change Password</kbd>. When prompted (twice), enter the new password on 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.

ⓘ   It is the responsibility of each assigned operator to use this service to change their own password. Refer to the TSM5XX Security Policy (Doc. No. PR-D2-0778) for further details on Cryptographic Officer and User roles.

3.15 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 the Crypto Officer to have logged in.

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

Click on <kbd>Force Tamper</kbd> 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

4 TsmWeb with STS Firmware

⚠️ **This section is only applicable to a TSM500i HSM with STS firmware.**

An HSM with STS or STS6 firmware has additional functionality provided via the STS Menu. For details on this additional functionality, refer to the following documents:

- TsmWeb-STS User Guide
- TsmWeb-STS Customisation

APPENDIX A – LCD SEQUENCE

Boot Menu


```
Boot Menu        ↑          ✓  ────►  Start Web server
1.Continue boot↓

Boot Menu        ↑          ✓         Edit addr? Y←  →N    ►N
2.IP Address     ↓                    001.002.003.004

                                      ◄Y
                                      Address (edit)      ✗
                                      _101.002.003.004

Boot Menu        ↑          ✓         ►N
3.Netmask        ↓                    101.202.303.404
                                      Save addr? Y←  →N

                                      ◄Y
                                      Store change

Boot Menu        ↑    ►N     ✓
4.Backup to USB↓        Confirm action  ◄Y  Perform backup

Boot Menu        ↑    ►N     ✓
5.USB restore    ↓      Confirm action  ◄Y  Restore NSS config &
                                            data from backup
                                            server's database

Boot Menu        ↑    ►N     ✓
6.Disable TLS    ↓      Confirm action  ◄Y  Disable TLS service

Boot Menu        ↑          ✓  ────►  Go to reset menu
7.Reset ...►     ↓
```
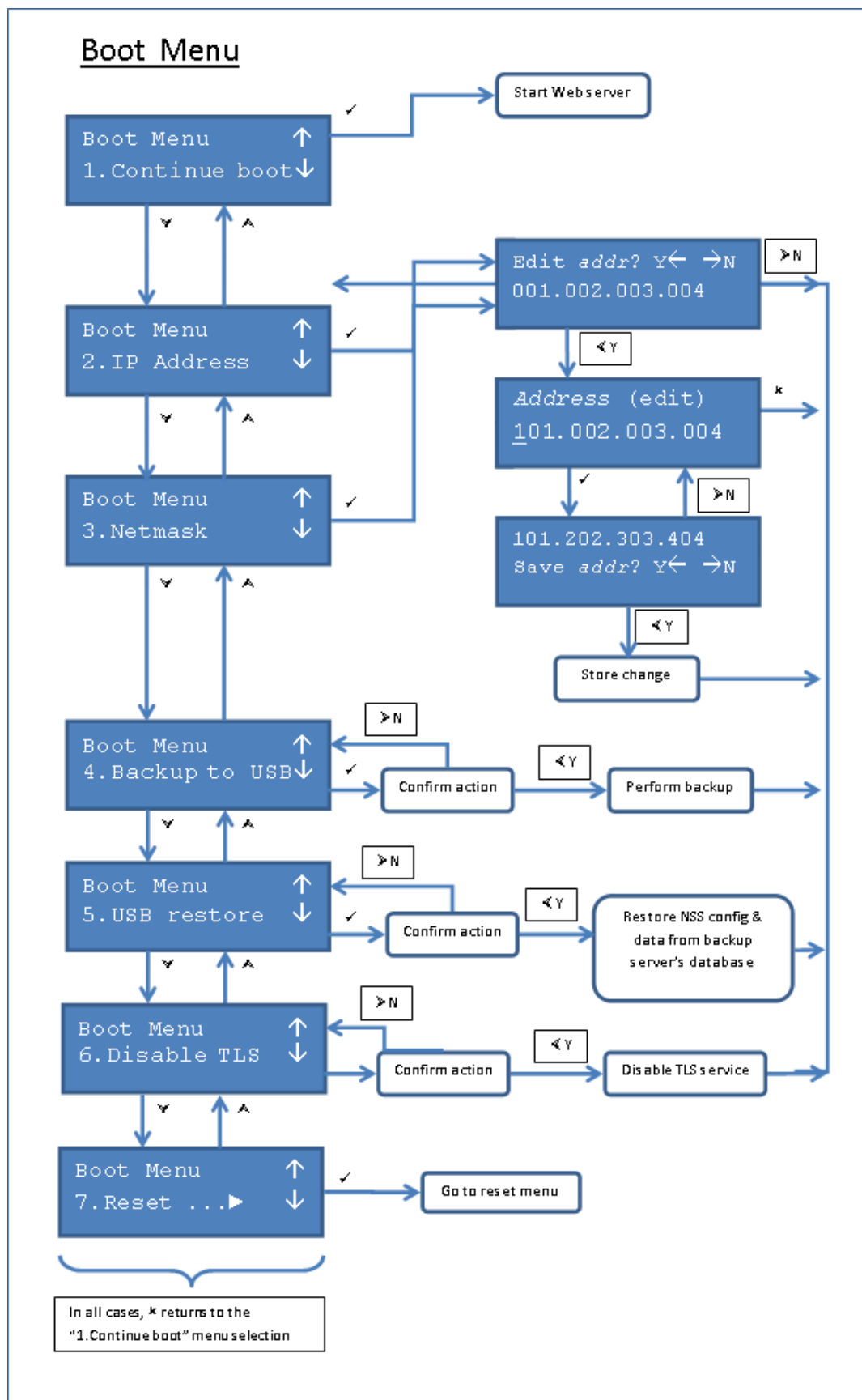
In all cases, ✗ returns to the
"1.Continue boot" menu selection

APPENDIX B – 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)
PCIe	PCI Express, a variant of PCI [2]
PCI HSM	HSM Security Standard set by PCI [1]
PIN	Personal Identification Number
POST	Power-On Self Test
SMK	Storage Master Key
TPS	Transactions Per Second
TSM500i	The hardware security module (HSM) described in this document
TSM500i-NSS	TSM500i integrated with an embedded computer system in 19" rack-mount case
TSM500i-PCIe	TSM500i with a PCIe interface for fitment into a PC
TSM-WEB	Management tool with web interface used for HSMs supplied by Prism