

TSM500i and TsmWeb User Guide (PCI HSM v3)

August 2022

Document number:	PR-D2-1037 Rev 1.6
Release date:	August 2022
Copyright:	© 2022 Prism Payment Technologies (Pty) Ltd
Synopsis:	This document describes the PCI HSM v3.0 TSM500i Hardware Security Module (HSM) as well as the TsmWeb interface used to manage this HSM.

Company Confidential

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

Disclaimer

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

Important Notes



This document only applies to a 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 following all of the appropriate security procedures detailed in Section 2.



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 2.8. 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.

Document Structure

This document comprises the following sections:

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.

Section 2 : Installation and Security Procedures

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

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

Section 3 : HSM Password Management

This section provides details on how to use and manage your crypto officer passwords on a TSM500i that is PCI HSM v3 certified.

Section 4 : Ongoing maintenance

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

Contents

1	TSM500i OVERVIEW.....	6
1.1	TSM500i-PCIe DESCRIPTION.....	6
1.2	TSM500i-NSS DESCRIPTION.....	6
1.3	KCED DESCRIPTION.....	7
2	INSTALLATION & SECURITY PROCEDURES.....	8
2.1	QUICK GUIDE: FROM INSTALLATION TO OPERATION.....	8
2.2	ESTABLISH SECURITY PROCEDURES.....	9
2.2.1	Security Awareness, and the implication of lost passwords and/or components.....	9
2.3	INSPECT AND INSTALL HARDWARE.....	11
2.3.1	Hardware Inspection.....	11
2.3.2	TSM500i-NSS Hardware Installation.....	11
2.3.3	TSM500i-PCIe Hardware Installation.....	12
2.4	CHECK PHYSICAL INDICATORS (LEDs).....	13
2.5	INSTALL DRIVERS, CONDUCTOR & TSM-WEB.....	14
2.6	NETWORK SETUP & RECOVERY.....	15
2.6.1	Use the LCD MENU to set the IP address.....	15
2.7	TSM-WEB INTERFACE.....	16
2.7.1	Invoking TSM-WEB for a TSM500i-PCIe.....	16
2.7.2	Invoking TSM-WEB for a TSM500i-NSS.....	16
2.7.3	Setting the TSM-WEB admin password.....	17
2.7.4	Using TSM-WEB for the first time.....	18
2.7.5	Accessing TSM-WEB through a different subnet.....	18
2.8	AUTHENTICATE HSM AND SET INITIAL PASSWORDS.....	19
2.8.1	Pairing the TSM500i HSM with the secure KCED over a local connection.....	19
2.8.2	Put the TSM500i into the Loader State.....	21
2.8.3	Authenticate HSM - Request Step.....	22
2.8.4	Authenticate HSM - Finalise Step.....	22
2.8.5	Add additional crypto officers.....	23
2.9	SET DATE AND TIME.....	24
2.9.1	[Optional Step] Set Date and Time.....	24
2.9.2	Put the TSM500i back into the Application State.....	24
2.10	CONFIGURING AND TESTING CONDUCTOR.....	25
2.10.1	Configuring Conductor on the TSM500i-NSS.....	25
2.10.2	Configuring Conductor on the TSM500i-PCIe.....	25

2.11	SETUP TSM-WEB ACCESS CONTROL	26
2.11.1	Create users	26
2.11.2	Configuring Account and Password Policy	26
2.11.3	Change Auto-Logoff Timeouts	26
2.11.4	Disable the default admin account	26
2.12	BACKUP NSS SETTINGS	27
2.13	PREPARE TSM FOR OPERATION: LOAD CSPs	28
2.13.1	Generating SMK components	28
2.13.2	Loading SMK components	29
2.13.3	[Optional] Setting the TSM500i HSM's Operational Permissions	30
2.14	CONFIGURING & TESTING CLIENT SOFTWARE	30
2.14.1	Generating and Loading Operational Keys	30
3	HSM PASSWORD MANAGEMENT	31
3.1	How to add a Crypto Officer	31
3.2	How to change an existing password	32
3.3	Reset One Password	33
3.4	Reset CSPs, clear all passwords, and set passwords	34
4	ONGOING MAINTENANCE	35
4.1	Check Operational vs Privileged state	35
4.2	Check Date & Time	35
4.3	Preference Manager	35
4.4	Storage Master Key Migration	36
4.4.1	Select SMK Migration tab and Login	36
4.4.2	Load a Migration SMK	36
4.4.3	Set the Migration SMK as the Active SMK	37
4.4.4	Delete the Migration SMK	37
4.5	TSM500i Status Information	38
4.6	NSS Log Files	38
4.7	NSS LCD Menu	39
4.8	Backup and Restore	40
4.8.1	Backup & Restore on a TSM500i-NSS	40
4.8.2	Backup & Restore on a TSM500i-PCIe	41
4.9	Reset NSS to Default Settings	42
4.9.1	Admin Passwd	42
4.9.2	Config Reset	42
4.9.3	Factory Reset	42

4.10	SSL/TLS Certificate.....	43
4.11	Disabling and Enabling SSL / TLS.....	43
4.11.1	Disable TLS from the LCD MENU.....	43
4.11.2	Disable or Enable TLS from TSM-WEB	43
4.12	Upgrading TSM500i firmware	44
4.13	Upgrading TSM500i-NSS System Software	45
4.14	Force a tamper condition	46
4.15	Clear tamper	47
5	REPAIRS.....	48
	APPENDIX A – LCD SEQUENCE.....	49
	APPENDIX B – LIST OF ABBREVIATIONS.....	55

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 only applies to a TSM500i that has Boot Loader v1.5.0.0 or later.**

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.

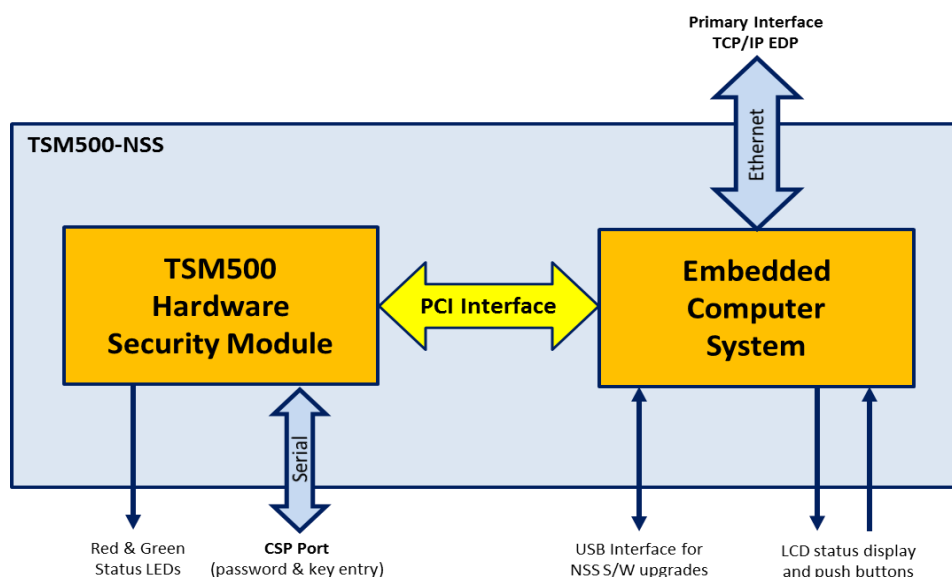


TSM500i-NSS v1.0 and v1.1



TSM500i-NSS v1.2

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 and section 3)
- Entry of Key Components (refer section 2.13)
- Generation of Key Components (refer section 2.13)

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-PCle, it connects to the RED port on the connector panel (this is the connector closest to the status LEDs).



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.

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



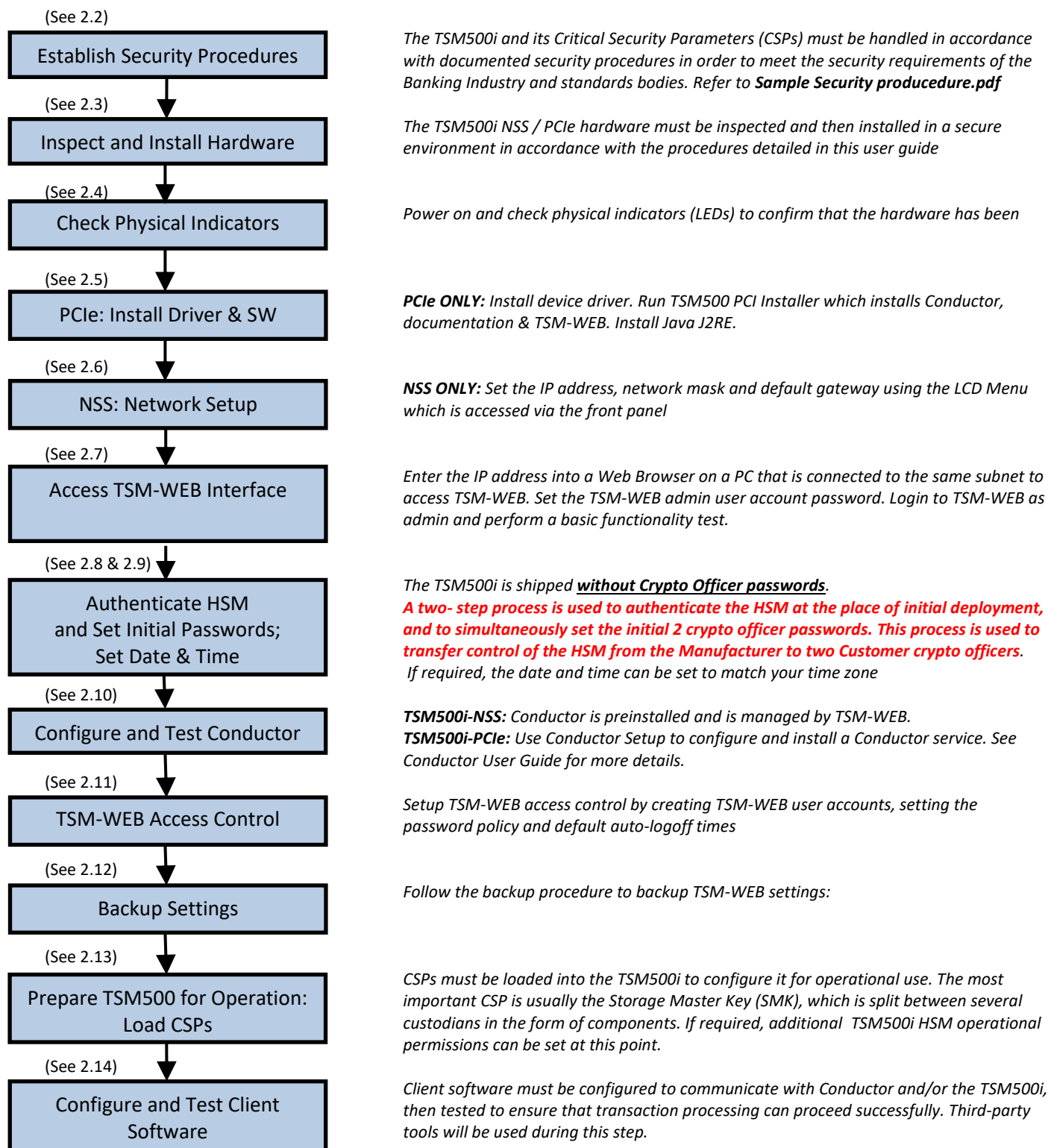
TSM500i-NSS v1.2: Single USB Port for Service and Local Secure KCED

The above photographs identify the connector to be used by the KCED on the TSM500i-PCle, the TSM500i-NSS (v1.0 and v1.1) and the TSM500i-NSS v1.2.

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.

2 INSTALLATION & SECURITY PROCEDURES

2.1 QUICK GUIDE: FROM INSTALLATION TO OPERATION



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.

2.2.1 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 both Ben and Collin (i.e. both crypto officers) forget their passwords then it will not be 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 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 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 that:-

- 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 their 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 recommend 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 to go through 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

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.
- 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.

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 **MUST** be used when not using an anti-static wrist strap.

- Ground yourself by making contact with the case of the machine for at least 2 seconds.
 - Limit your movements as to prevent excessive build-up of static electricity.
 - 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-PCle is installed.



The red and green Status LEDs provide very important information about the current state of the TSM500i.

- For the TSM500i-NSS, the status LEDs are located on the front panel
- For the TSM500i-PCle, 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 TSM500i-PCIe (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 TSM500i-NSS (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 *LCD MAIN 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 LCD Main 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 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 [APPENDIX A – LCD SEQUENCE](#).

2.7 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-PCle

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

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).

The screenshot shows a web browser window displaying the TSM-Web TSM Status page. The browser's address bar shows the URL <https://192.168.0.220/nss/>. The page has a blue header with the PRISM logo and the text 'TSM-Web TSM Status'. A sidebar on the left contains a navigation menu with items like HOME, SYSTEM, NETWORK SETTINGS, CONDUCTOR SETTINGS, TSM, ACTIVITY, ALERTS, LICENSES, MIGRATE, PREFERENCE MANAGER, REPORTS, USERS, LOGS, and DOCUMENTATION. The main content area is titled 'TsmWeb-NSS' and displays various system parameters in a table-like format.

TsmWeb-NSS	
Version	4.53.0
Up since	2018-05-31 10:03:42
Network	
Network address	192.168.0.220
TLS certificate expiry	2019-10-25 (CCYY-MM-DD) 14:54:00
TSM	
TSM family	TSM500
TSM UID	7179A66C01000066
TSM firmware	MCM v4.0.0.0
Performance rating	TPS:600
Real-time clock	DATETIME:20180605T152853Z
Access control mode	AC:OPERATIONAL
Conductor	
Conductor service	running
Conductor port	5100
Conductor versions	conductor 1.3.14 edp 1.3 DcmNtDrv.dll 3.2.7.0 TSM500Drv 3.3.15.0 tsm500_wd 10.4.0.0
Web Interface	
Web UI port	443 (80)
Web service port	8080

Generated at 2018-06-05 15:26:32 by TsmWeb-NSS v4.53.0 in 36.006ms on NSSPRIS-9N7U05L

2.7.3 Setting the TSM-WEB admin password



*User / Password Setup is optional on a TSM500i-PCle when using TSM-WEB from the computer that hosts the TSM500i-PCle. To login on a local installation, click **Login as \$Local**. When accessing the TSM500-PCle from a remote computer, it process is the same as for the TSM500i-NSS which means TSM-WEB user accounts will need to be setup as detailed below.*

Please note that TSM-WEB is not supplied with default passwords and it is necessary to set a password 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 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 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. 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.



TSM-WEB will automatically log the user off after a default of 10 minutes of inactivity. This timeout period can be configured via *Preference Manager* page on TSM-WEB.



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 2.11 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 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 2 crypto 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 TSM-WEB user account passwords.

TSM500i HSM shipped with V1.6.0.0 (or later) Boot loader and V5.0.0.0 (or later) Application firmware then it requires a secure KCED. The Secure KCED firmware must be V3.50 (or later).

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.

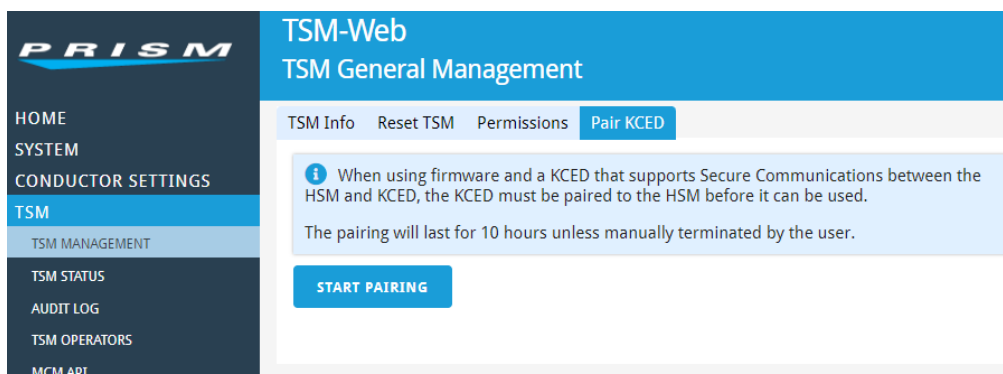
Requirements: Logged into TSM-WEB and the KCED connected to the TSM500i.

2.8.1 Pairing the TSM500i HSM with the secure KCED over a local connection

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

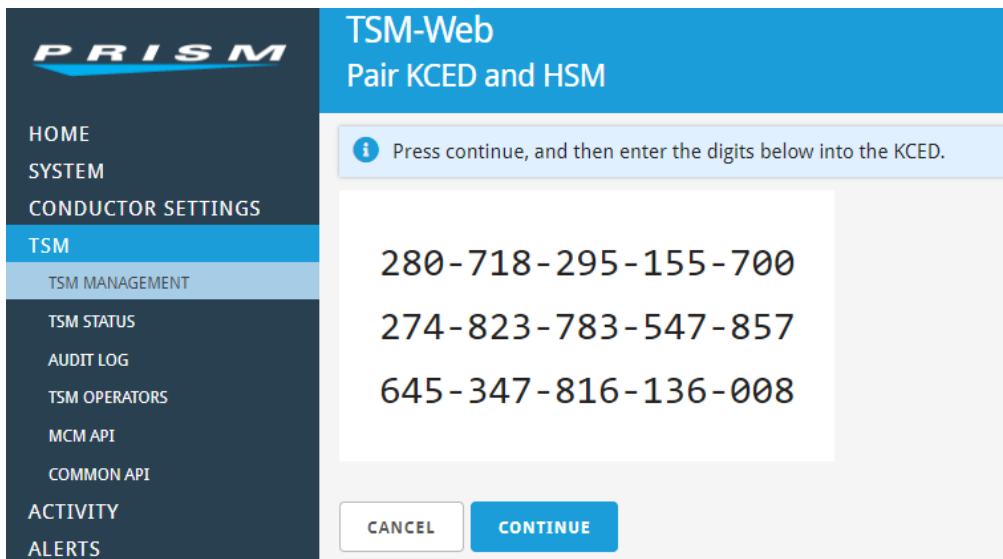


Pairing is not applicable with TSM500i HSMs that have Boot loader earlier than V1.6.0.0 and application firmware earlier than V5.0.0.0.

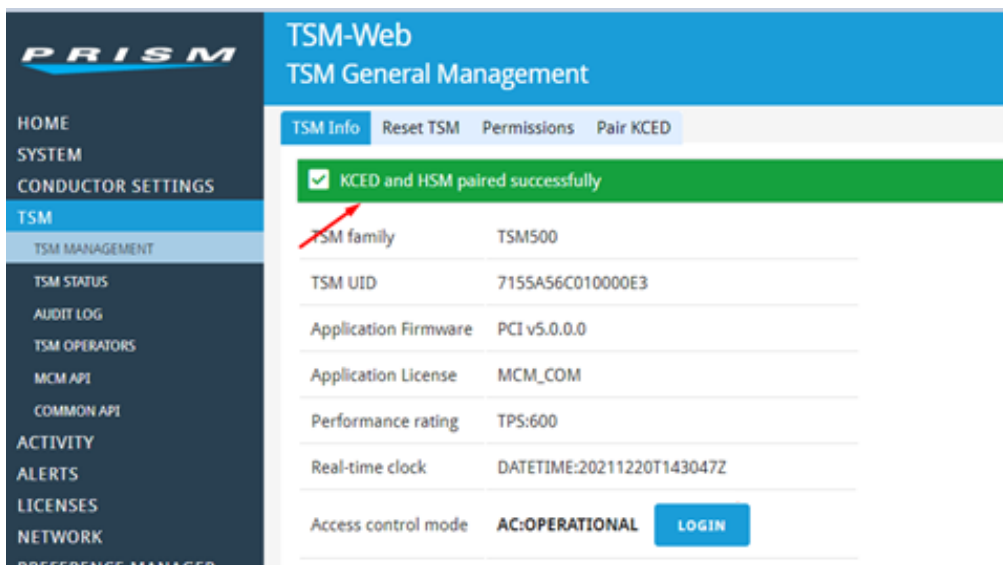


Under “Pair KCED” click on “START PAIRING” button

The HSM will generate its random key pair and a 45 digit fingerprint (pertaining to its public key), which is then displayed on TsmWeb. Click on “CONTINUE”



The KCED will solicit the entry of the HSM's public key fingerprint at this point. 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 Application state 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 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 been terminated then the TSM500i HSM and the KCED will need to be repaired if further use of the KCED is required.

2.8.2 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 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.

2.8.3 Authenticate HSM - Request Step

- On the **TSM Operators** page click on “Authenticate HSM and Set Initial Passwords” tab.
- Select “Request” from the “Action” drop down menu. Click on **REQUEST**.
- 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. Sample wording for the request is provided in a template on the support CD that is provided with the HSM.



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 in response to the last challenge issued.

2.8.4 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 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 **FINALISE**.
 - 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.

2.8.5 Add additional crypto officers

Refer to section 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.

2.9 SET DATE AND TIME

2.9.1 [Optional Step] Set Date and Time

Requirements: Logged into TSM-WEB 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 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.

2.9.2 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 TSM" tab on the **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.

2.10 CONFIGURING AND TESTING CONDUCTOR

2.10.1 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 the Conductor TCP Port (default 5100) is enabled for incoming connections on the firewall.

2.10.1.1 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.

2.10.1.2 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.

2.10.1.3 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.

2.10.1.4 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.

2.10.2 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.

2.11 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.

2.11.1 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.

2.11.2 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](#).

2.11.3 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

2.11.4 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'.

2.12 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 MAIN MENU.

- 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 [APPENDIX A – LCD SEQUENCE](#) for a flow chart of the menu functions.
- Scroll down to Backup to USB option on the MAIN MENU and press the green ✔ button to select. Confirm using the left arrow button.
- Once the backup is complete you will be given the option to continue the boot process. Press the green ✔ button to continue.

Special requirement for backing up large databases

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

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

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

2.13 PREPARE TSM FOR OPERATION: LOAD CSPs



This section covers operational preparation for all TSM500i HSMs except 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.

2.13.1 Generating SMK components

This service is only available when the TSM500i is in the *Privileged* mode. The TSM500i may need to be paired with the secure KCED before it can be placed into 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 **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

- 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.

2.13.2 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”. An AES-KB SMK is recommended
- 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.



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.

2.13.3 [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 Management** 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.

2.14 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.

2.14.1 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 2.13.1 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. The TSM500i may need to be paired with the secure KCED before it can be placed into the *Privileged* mode.

3 HSM PASSWORD MANAGEMENT



This section is not applicable to TSM500i HSMs running STS64Vxx firmware.

3.1 How to add a Crypto Officer

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!



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.

Requirements:

- Logged into TSM-WEB 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 “Manage Operators” tab on the **TSM Operators** page.
- To add an operator check “NEW OPERATOR”.
- Set the “NAME” field with the name of the new officer. Click on **ADD OPERATOR**.
- Follow the on screen instructions on the KCED. When prompted (twice), enter the new password on the KCED.
- 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!**



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

3.2 How to change an existing password



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

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

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



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.

- Click on “Manage Operators” tab on the **TSM Operators** page.
- To change a password, select the appropriate *Operator ID*.
- Set the “Name” field with the details of crypto officer. Click on **CHANGE PASSWORD**.
- Follow the on screen instructions on the KCED. When prompted (twice), enter the new password on the KCED.
- 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!**



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

3.3 Reset One Password



This operation may be used to **RESET** one password. It requires a **reset certificate from the Manufacturer** and it also requires **one 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 TSM-WEB 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** whereafter they will not function.



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.

Process:

- Click on “Reset Password” tab on the **TSM Operators** page.
- Set “Operator Name” field.
- Copy the token that was received from the Manufacturer into the box and click.
- The Crypto Officer must look at the **KCED screen** that should show a message for Operator to enter a new password. **The password must be entered via the KCED keypad.**
- Follow the on screen instructions on the KCED. When prompted (twice), enter the new password on the KCED.
- 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!**



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

3.4 Reset CSPs, clear all passwords, and set passwords

This operation should NOT be used to set initial passwords - for that use 'Authenticate HSM & Set Initial Passwords' (see section 2.8).

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 TSM-WEB 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.



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.

Process:

- Click on "Clear CSPs and Reset Passwords" tab on the **TSM Operators** page.
- Set "Officer 1 Name" and "Officer 2 Name" fields.
- Copy both tokens into their respective boxes and click on **CLEAR CSPS & RESET PASSWORDS**.
- 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.
- 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!**



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

4 ONGOING MAINTENANCE

4.1 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 not left in the Privileged state after operations requiring dual control. The HSM 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.

4.2 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 2.9 will set both clocks simultaneously.

4.3 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 is done (see section 2.12) all the preferences are included in the backup.

4.4 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 2.13.2.

4.4.1 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.

4.4.2 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.

4.4.3 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.

4.4.4 Delete the Migration SMK

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

4.5 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.

Select the **TSM Status** page from within the **TSM** menu 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.

4.6 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.

4.7 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 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, default gateway | - refer to section 2.6.1 |
| • USB Backup & Restore | - refer to section 2.12 |
| • Reset to Defaults | - refer to section 4.9 |
| • Disable SSL/TLS, reset TLS key | - refer to section 4.11 |

4.8 Backup and Restore

4.8.1 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 2.12 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.

- *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 [APPENDIX A – LCD SEQUENCE](#) for a flow chart of the menu functions. This takes approximately 20 seconds.
- Scroll down to USB Restore option on the MAIN MENU and press the green ✓ button to select. Confirm using the left arrow button. The message ‘NSS Restore’ is displayed followed by NSS Restore – Success.
- Wait for the Main Menu to appear on the LCD. Select Continue Reboot.

Additional considerations for restoring a backup to a different NSS

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

- *An NSS backup must be restored to an NSS with the same (or higher) firmware version.*
- Network settings are restored, so the restored NSS will have the same IP address as the backed up NSS. When restoring to a different NSS you should physically disconnect the NSS from the network before restoring; then use the NSS LCD Menu (4.7) 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.

4.8.2 Backup & Restore on a TSM500i-PCle



*This procedure is only applicable to the **TSM500i-PCle** (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.

4.9 Reset NSS to Default Settings

Section 4.7 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:

4.9.1 Admin Passwd

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 2.7.3.1.

4.9.2 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”)

4.9.3 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”.

4.10 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.

4.11 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.

4.11.1 Disable TLS from the LCD MENU

Using the LCD MAIN MENU as described in section 4.7, select the “Disable TLS” option and confirm the operation. The TLS service is now disabled.

4.11.2 Disable or Enable TLS from TSM-WEB

TLS cannot be re-enabled via the LCD 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.

4.12 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_OFFICER if loading firmware of same type & later version

BL:LOADER_ROLE_DUAL_OFFICER if loading firmware of different type or earlier version

Click on “Update Firmware” tab on 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 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.

4.13 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:

- *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.

4.14 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 both Crypto Officers to have logged in.

i.e. *Access Control Mode* **must** be **BL:LOADER_ROLE_DUAL_OFFICER**

Click on **Tamper** tab.

Click on **Force Tamper** 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

4.15 Clear tamper

If the TSM500i is in a tampered state you will need to reset the tamper. This service requires both 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, select the **TSM Status** page from the side menu 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.

On the **TSM Management** page click on **Tamper** tab. Click on **Clear tamper** to clear the tamper. Verify that the RED LED turns off.

5 REPAIRS

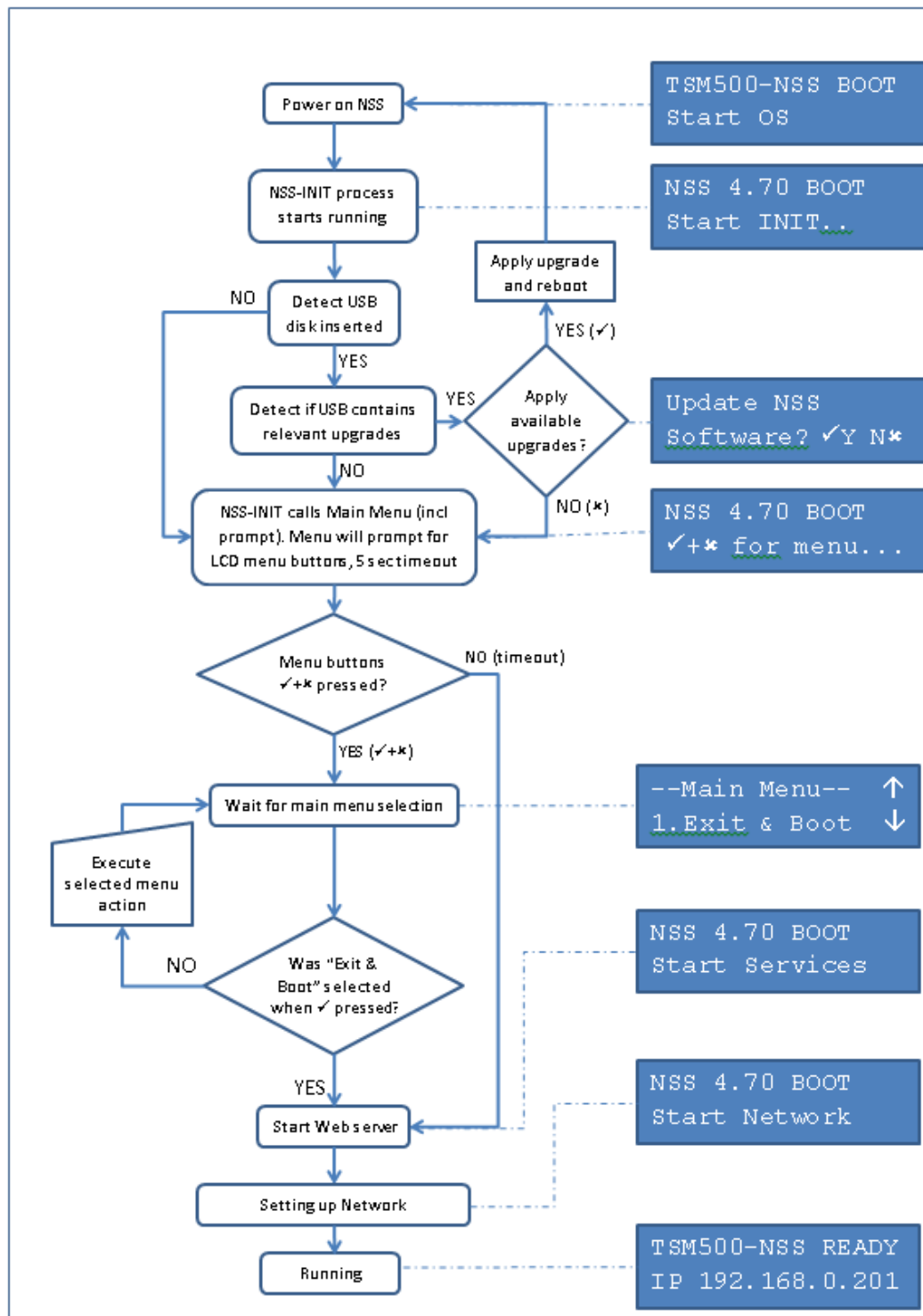
The TSM500i has no user-serviceable parts. Opening the lid and/or removing the tamper stickers on the side of the HSM is a security breach. In addition, it will void the warranty on the product.

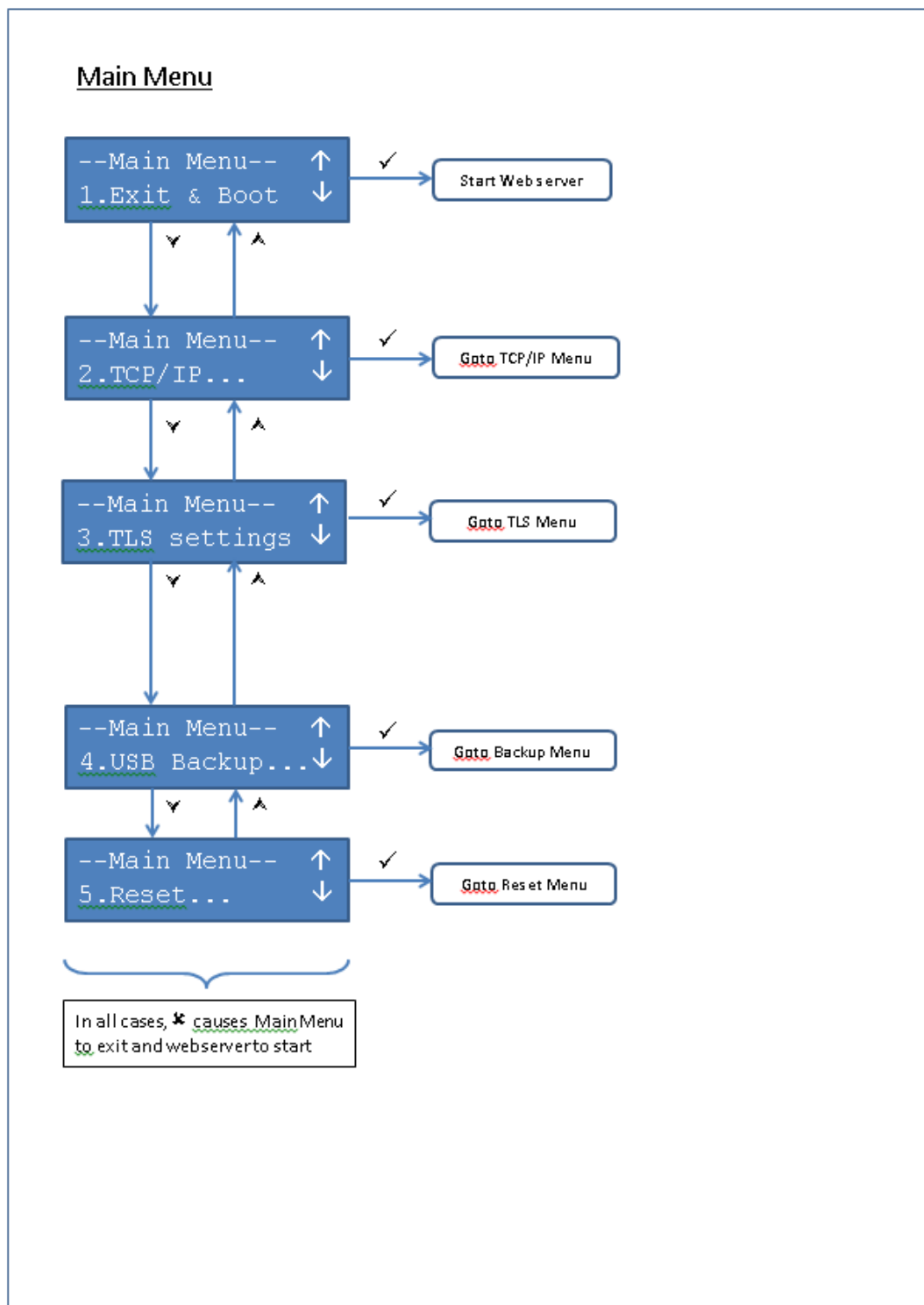
In the event of a fault that cannot be resolved remotely, the HSM must be returned to the Manufacturer (Prism Payment Technologies Pty Ltd) for repair.

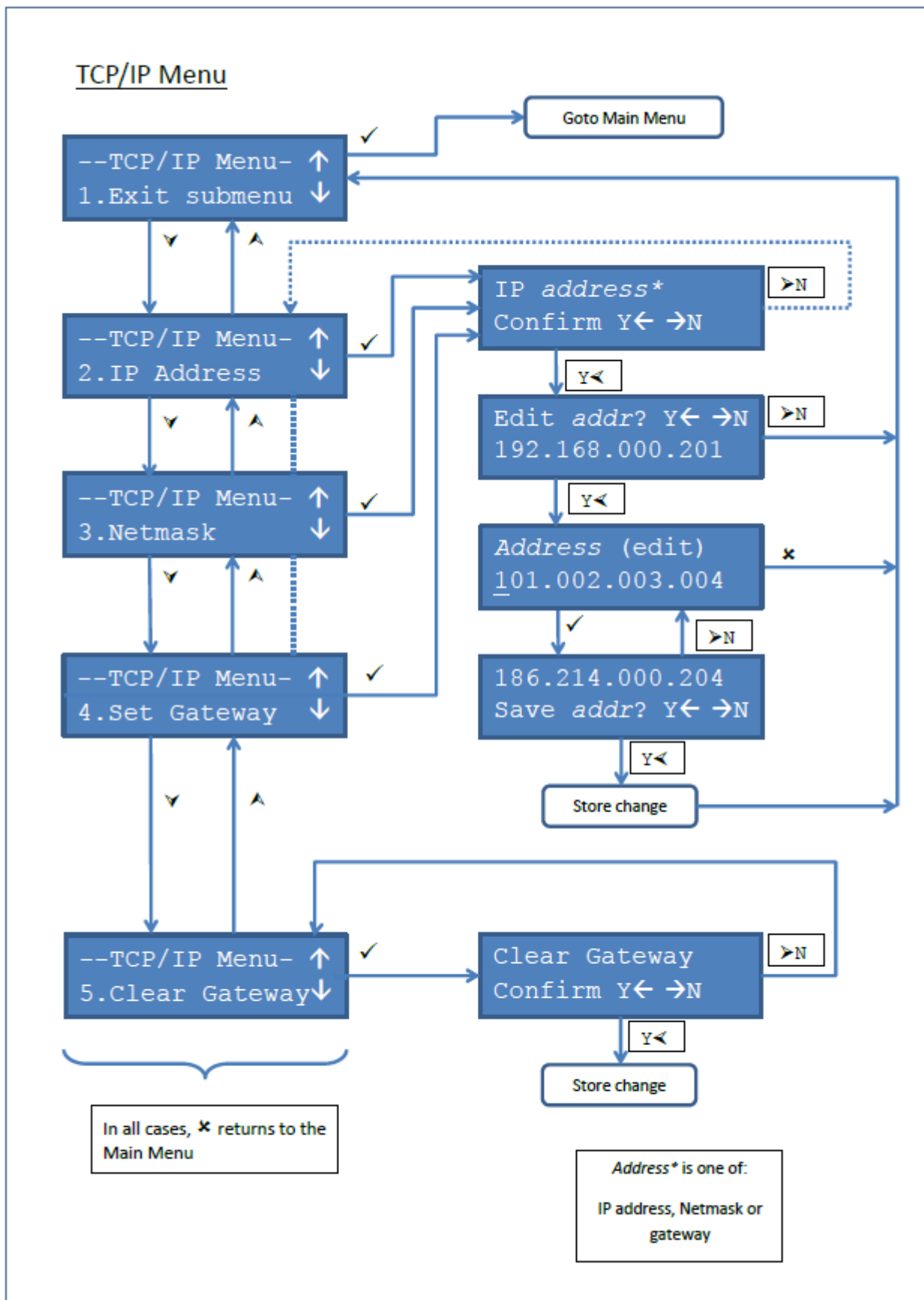
Battery Replacement:

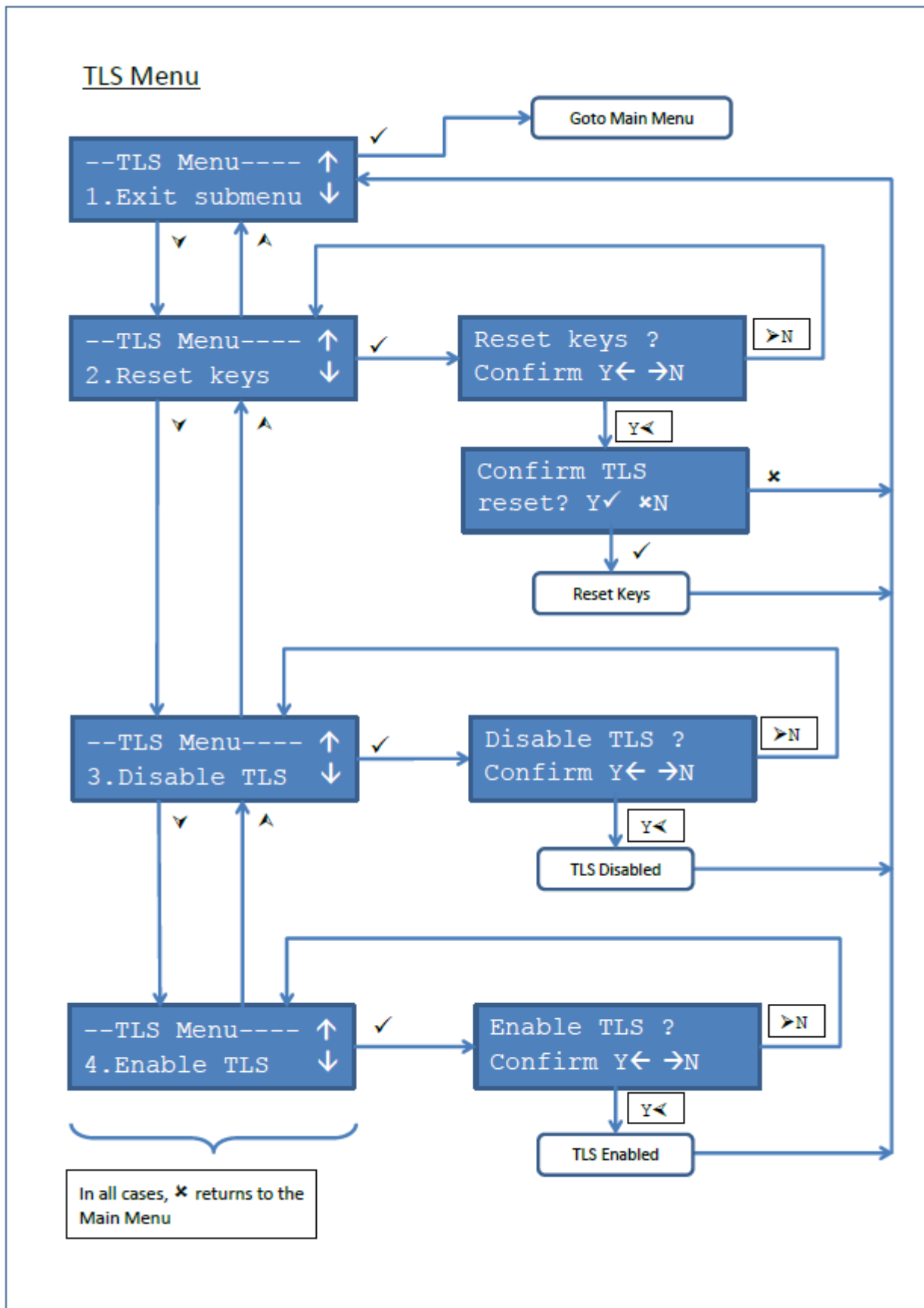
The internal batteries have a life expectancy of more than 10 years. In line with the above statement, the batteries can only be replaced by the Manufacturer.

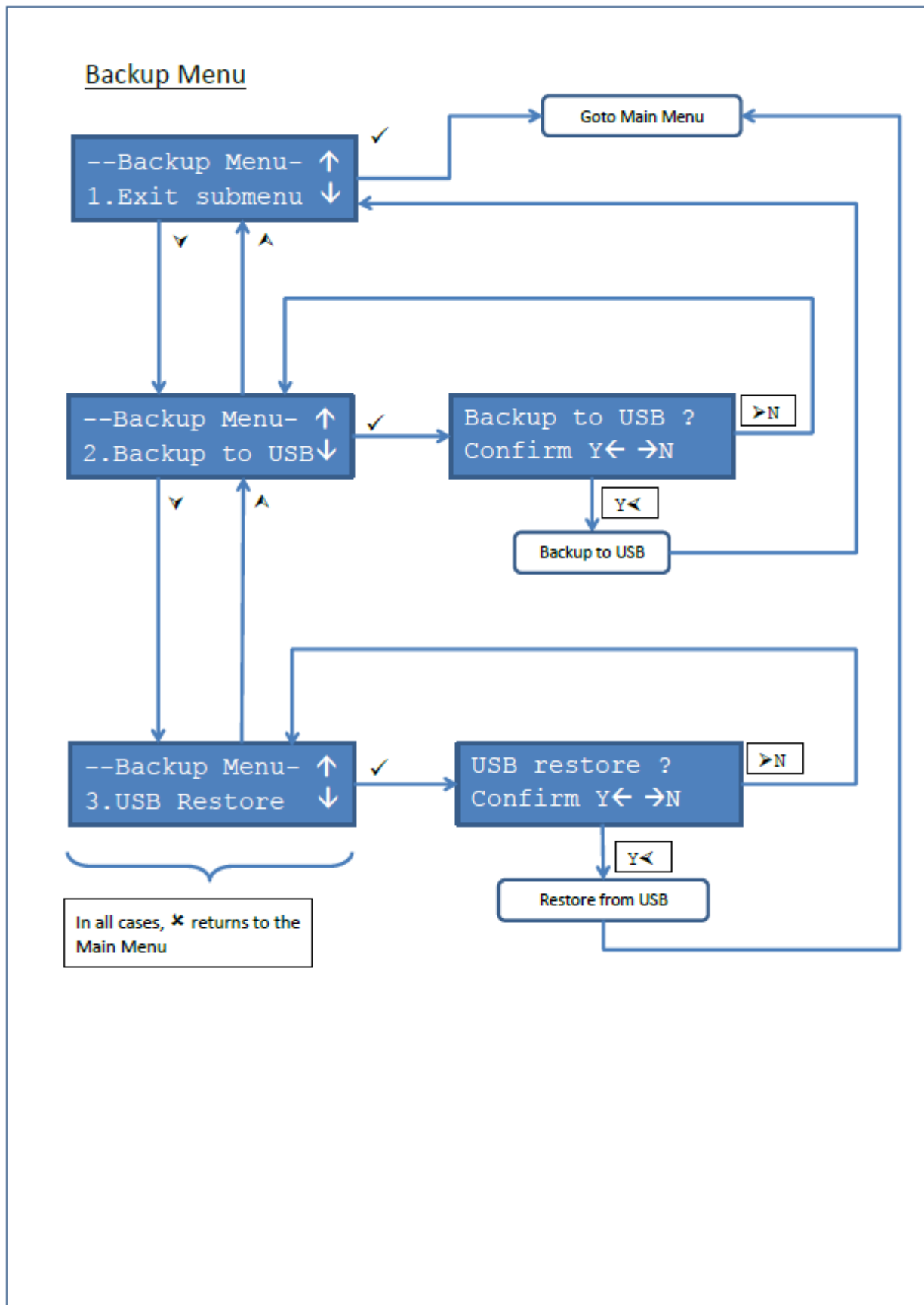
APPENDIX A – LCD SEQUENCE

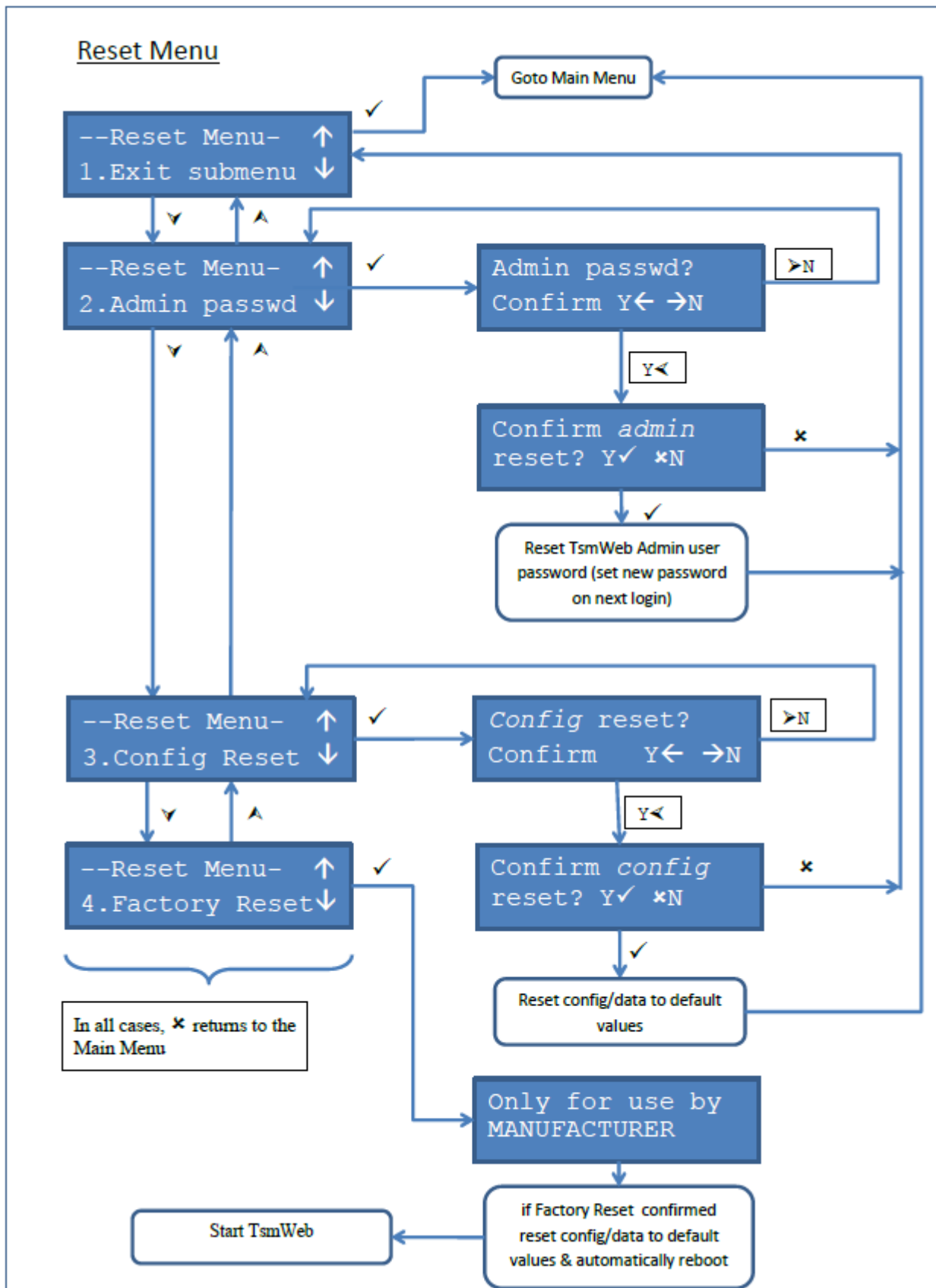












APPENDIX B – LIST OF ABBREVIATIONS

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