The Prism TSM500 series Hardware Security Modules (HSM) offer an affordable high-security solution for issuers, processors/switches, acquirers and mobile network operators in the electronic payments industry.

**Certification**

Prism’s TSM500 series tamper responsive/resistant HSMs are certified to **FIPS 140-2 level 3** or **PCI HSM v2.0**.

**Channel Compatibility**

The TSM500 series HSMs provide transaction processing services via TCP/IP over an Ethernet interface. They are plug-in compatible with Postilion and Traderoot software.

**Excellent Price and Performance Value**

Available in a range of models from 20 TDES PIN translations per second upwards offering the best price/performance value in the industry. All TSM500 series HSMs models are performance upgradeable at your premises. You can purchase a crypto solution that is suited to your existing processing needs, upgrade performance as required, ensuring you only pay for the performance you require.

**Ease of Use**

With the comprehensive documentation supplied, it is a straightforward process to manage and configure the TSM500 series HSMs using a web browser based interface.

**Service and Support**

Prism provides a 1 year hardware warranty with the option of an extended hardware warranty or service agreement.
**SPECIFICATIONS (TSM500 Series)**

**Certification / Validation**
- TSM500 - FIPS 140-2 level 3 (Cert#1292)
- TSM500i - PCI HSM v2.0 (Approval# 4-60158)

**Price/Performance**
- Field upgradable from 20 Triple DES PIN translations per second upwards

**Network Access**
- Communication with HSM API is performed using a datagram protocol over TCP/IPv4
- The same network service is used across the HSM range

**Access Control and Key Loading**
- Built-in access control enforces dual control for sensitive operations, such as, key loading
- Appointed security officers enter their passwords using the Key Component Entry Device to authorise such operations
- Key components are entered directly into the TSM500i via a Key Component Entry Device

**External hardware requirements**
Prism Key Component Entry Device for access control and loading key components

**SDKs and Custom Firmware Development**
- SDKs are available
- Prism can develop firmware to meet your requirements
- Please contact us for further information

**Environmental Characteristics**
- Operating temperature: 2 - 40 °C
- Relative humidity: 5 – 95% (non-condensing)
- RoHS compliant (free of hazardous substances)

**Model: TSM500-NSS/TSM500i-NSS**
**Form Factor: 19” Rack Mount Appliance**

**Dimensions**
- 483mm width, 175mm depth, 1U height

**Interfaces**
- Gigabit (10/100/1000 Mbps) Ethernet port
- Primary serial port for key component entry
- Secondary serial port (e.g. for serial printers)
- USB service port

**Platforms**
- All platforms that can communicate over TCP/IP

**Physical Characteristics**
- Input Voltage: 100 – 240V AC 50-60Hz
- Power consumption: 30W (maximum)
- Weight: 2.5Kg

**Banking and EFT System Features**
- PIN translation
  - Schemes: DUKPT and Master/Session
  - Formats: ISO 9564/X9.8 formats 0, 1 & 3
- PIN verification (IBM/3624 PIN Offset, Visa PVV)
- Card verification (CVV, CVV2, CVC)
- MAC generation and verification
  - ANSI double-key retail MAC (X9.19)
  - ISO 9797-1 Algorithm 3
- Key Block formats for interoperability
  - X9 TR-31 & AKB are supported
- Management of encrypted keys compatible with X9.24-1, X9.24-2 and ISO-11568
- EMV v3.x & v4.x transaction processing and secure messaging (with PIN change)
- Data encryption/decryption support for PCI DSS
- Authenticated message encryption for P2PE
- Remote key loading / distribution to PEDs/ATMs
- Audit trail

**Algorithms**
- DES and Triple TDES (TDES) algorithms
- AES algorithm (FIPS 197)
- RSA key generation, signing and verification support for key lengths up to 2048 bits (X9.31)
- SHA hash algorithms (ISO 10118/FIPS 180-4)
- HMAC (FIPS 198-1)

**mCommerce System Features**
- Mobile security extensions for SMS and mCommerce security
- Includes most features detailed above

**Supported Standards**
- FIPS: 180-4, 186, 197, 198-1
- ISO: 9564, 10118, 11568, 13491
- ANSI: X9 TG-39, TR-31

**Model: TSM500-PCIE/TSM500i-PCIE**
**Form Factor: PCI Express adapter card**

**Dimensions**
- 209mm length, 111mm height

**Interfaces**
- PCI Express x1 (functions in x4, x8 & x16 slots)
- Primary serial port for key component entry
- Secondary serial port (e.g. for serial printers)

**Platforms**
- Microsoft Windows 2008 R2 (64 bit)
- Microsoft Windows 2008 (32 bit & 64 bit)
- Microsoft Windows 2003 (32 bit)
- Microsoft Windows 7 (64 bit)
- Microsoft Windows Vista (32 bit & 64 bit)

---

**Disclaimer:** The material in this document is presented strictly for information purposes. While every effort has been made to ensure its correctness, neither the correctness nor the suitability of the information for any purpose is warranted. Product specifications and features are subject to change without notice. Copyright Prism Payment Technologies (Pty) Ltd. All rights reserved.