TSM500i HSM DATASHEET

Hardware Security Module for Payments

The Prism range of Hardware Security Modules (HSM) offer an affordable high-security solution for issuers, processors/switches, acquirers and mobile network operators in the electronic payments industry since 1996.

Certification

- Proven Hardware Security Modules (HSM) that are tried, tested and trusted!
- Prism's TSM500i tamper responsive/resistant HSMs are certified to PCI HSM v3.0

Channel Compatibility

The TSM500i HSMs provide transaction processing services via TCP/IP over an Ethernet interface. They are plug-in compatible with Postilion, Traderoot, iZealiant Access Control Server (ACS) and PayTabs SwitchOn 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 TSM500i 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 TSM500i HSMs using a web browser based interface.

Disclaimer: The material in this document is presented strictly for infomation purposes. While every effort has been made to ensure it's correctness, neither the correctness nor the suitability of the infomation for any purpose is warranted. Product specifications and features are subject to change without notice.

Prism's products and solutions provide key technology and secure transaction processing for prepayment vending, EFT and mCommerce markets.

As industry leaders with over 25 years' experience, we have produced a number of award-winning Hardware Security Modules and systems primarily aimed at the financial, retail, telecommunications and utilities sectors. We continually strive towards building on our experience and expertise enabling us to not only meet security standards but define them.

Specifications

Prism provides a 1 year hardware warranty with the option of an extended hardware warranty or service agreement.

Certification / Validation

- TSM500i - PCI HSM v3.0 (Approval # 4 - 20327)

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)

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 (KCED) for access control and loading key components

Tutorials & Custom Firmware Development

- SDKs/Tutorials are available
- Prism can develop firmware to meet your requirements
- Please contact us for further information

Environmental and Safety Characteristics

- Operating temperature: 2 – 40 °C
- Relative humidity: 5 – 95% (non-condensing)
- RoHS compliant (free of hazardous substances)
- Compliant with IEC 62368-1 safety requirements
- Compliant with EN 55032 & EN 55035 standards

Banking and EFT System Features

- PIN translation (AES & TDES DUKPT & Master/Session)
- Formats: ISO 9564/X9.8 formats 0, 1, 3 & 4
- PIN verification (IBM-3624 PIN Offset, Visa PVV)
- Card verification (CVV, CVV2, CVC)
- Dynamic CVV (CVC3)
- MAC generation and verification
- ANSI double-key X9.19, ISO 9797-1 Alg 3
- X9 TR-31 & AKB Key Block formats are supported
- Management of encrypted keys compatible with X9.24.1, X9.24-2, X9.24.3 and ISO-11568
- EMV v3.x & v4.x transaction processing and secure messaging (with PIN change)
- TDES & AES data encryption/decryption support for PCI DSS
- P2PE support (TDES DUKPT & BPS)
- Remote key loading / distribution to PEDs/ATMs
- Audit trail

Algorithms

- DES and Triple TDES (TDES) algorithms
- AES algorithm (FIPS 197)
- BPS Format Preserving Encryption (FPE)
- RSA (up to 4096 bit X9.31) key generation, signing & verification
- ECC (P-224 to P-521) key generation, signing & verification
- 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

- ANSI: ANS X9.8, X9.19, X9.24, X9.31, X9.52
- FIPS: 180-4, 186-4, 197, 198-1
- ISO: 9564, 10118, 11568, 13491, 20038
- ANSI: X9 TG-39, TR-31

Model: TSM500i-NSS

Form Factor: 19” Rack Mount Appliance

Dimensions

- 483mm width, 250mm depth, 1U height

Interfaces

- Gigabit (10/100/1000 Mbps) Ethernet port
- Secondary serial port (e.g. for serial printers)
- USB port for software upgrades & KCED

Platforms

- All platforms that can communicate over TCP/IP

Physical Characteristics

- Input Voltage: 100 – 240V AC 50-60Hz
- Power consumption: 50W (maximum)
- Weight: 4.65kg

Model: 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

- Windows Server 2016
- Windows Server 2012 and 2012 R2
- Windows Server 2008 and 2008 R2
- Windows Server 2003
- Windows 7, 8 and 10