



P3™

Cryptographic Module P3CM-250

KEY BENEFITS

- > Optimized for card issuance applications
- > Cost effective and field upgradable functionality
- > Flexible form factor for desktop or rack mount use
- > Always up to date with latest EMV specifications
- > FIPS 140-2 Level 3 certified solution

The P3CM-250 is a high performance hardware cryptographic module optimized for use with the P3 data preparation software, providing the cryptographic functions required for key management, key generation, message authentication and smart card EMV data preparation in real time.



> P3™

Technical specifications

Cables

The P3CM is shipped with the following:

- > Power cable (region specific)
- > 9-way to 9-way RS-232 console cable
- > 26-way to 9-way RS-232 host cable

Cryptographic support

The P3CM supports the following cryptographic algorithms:

- > DES and Triple DES
- > RSA 512 to 2048 bits
- > SHA-1
- > MD5

Local Master Key Components are stored on smart cards (ISO 7816) for secure storage or distribution.

EMV application support

The P3CM includes optimized cryptographic support for the following card association applications on a range of smart card platforms:

- > **American Express** – AEIPS, ExpressPay
- > **Discover** – D-PAS, ZIP
- > **JCB** – J/Smart, J/Speedy
- > **MasterCard** – M/Chip Lite, M/Chip 2 Select, M/Chip 4, M/Chip Flex, M/Chip Advance, PayPass
- > **Saudi Arabian Monetary Agency (SAMA)** – SPAN2
- > **Union Pay** – PBOC
- > **Visa** – VSDC (SDA or DDA), qVSDC, MSD, VMFA, payWave

Communications interfaces

The P3CM supports the following host communication interfaces:

- > TCP/IP (Ethernet)
- > RS-232 (Asynchronous/serial)

Tamper evidence/resistance

Robust metal enclosure providing resilience against physical damage and attack.

Security labels on outside casing to indicate attempts to open the box. The tamper evident labels are under strict control of Thales and cannot be purchased on the open market.

A hole on the rear panel supports a Kensington lock for added security when used in surface/desktop mode.

Security certification

The P3CM utilizes the Thales Secure Generic Sub-System (SGSS) for all its cryptographic and security processing. This sub-system is validated to FIPS 140-2 level 3.

Power

Voltage: 100 to 240 V

Frequency: 47 to 63 Hz

Consumption: 1.0 - 0.6 A

Storage temperature

-10°C to 50°C (14°F to 122°F).

Operating temperature

The maximum ambient operating temperature for the P3CM is 40°C.

If using the P3CM in an enclosed environment the ambient temperature inside the enclosure must not exceed the stated maximum.

Relative humidity

10% to 90% at 25°C (77°) non-condensing, falling to 50% maximum at 40°C (100°F).

Barometric pressure

780 to 1100 mBar.

Dimensions

19" rack mounting brackets

	With	Without
Height:	44mm (1U)	44mm (1U)
Width:	482mm	400mm
Depth:	225mm*	225mm*

*243mm including earthing stud.

The P3CM is suitable for rack mounting or resting on a horizontal surface (e.g. a shelf or desk).

Performance

Highly scalable performance possible by deploying multiple P3CMs with P3 (Server). Key caching support offered by P3CM dramatically increases DDA application data preparation performance.