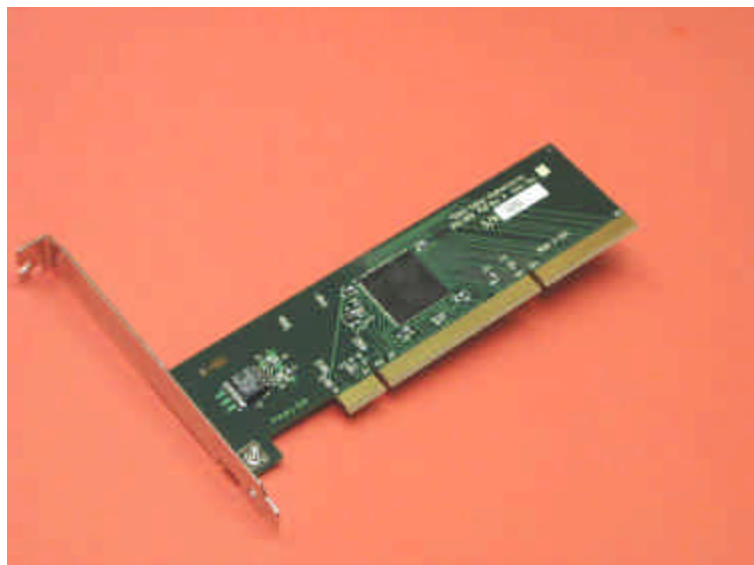# ZPCI.3910

MPC190 Security Processor PCI Card

Security Processor optimized for IPsec, IKE, WTLS/WAP, SSL/TLS

3.3V 33/66 MHz 64-bit PCI Interface

High-performance Bus-master Design

PCI rev 2.2 compliant

- **6 Public key execution units that perform:**
  - **Modular arithmetic and exponentiation with 80 to 2048-bit field size supports RSA and Diffie-Hellman**
  - **Elliptic curve operations with 55 to 511-bit field size support F_P and F_2m**
- **3 Data encryption standard execution units that perform:**
  - **DES in ECB or CBC modes**
  - **3DES in two key (K1, K2, K1) or three key (K1, K2, K3) ECB/CBC modes**
- **3 Message digest execution units that perform:**
  - **MD4 (128-bit)**
  - **MD5 (128-bit)**
  - **SHA-1 (160-bit)**
  - **HMAC-MD5 and HMAC-SHA-1**
- **ARC four execution unit that performs:**
  - **RC4 compatible stream cipher with a 40 to 128-bit key**
- **Random number generator**
- **9 Crypto-channels, each with multi-command descriptor chain support**
- **PCI rev 2.2 compliant master/slave**
- **3.3V Low-power design (2W typical)**
- **On-board 1.8V regulator**
- **Software and development support**

The **ZPCI.3910** MPC190 Security Processor PCI card from Zephyr Engineering, Inc is a high-performance encryption/decryption engine on a 3.3V 64-bit 66 MHz PCI card.

High Performance

The **ZPCI.3910** MPC190 Security Processor PCI card is capable of performing 3DES encryption/decryption at rates of up to 0.68 Gbps and MD5 authentication at 0.97 Gbps.

PCI Form Factor Gives You System Flexibility

You can plug the **ZPCI.3910** into any 3.3V PCI slot. Install it in your PC along with a standard PCI ethernet card and you have a complete security processor system.

Public Key Hardware Accelerators (PKHA)

Each of the six **ZPCI.3910** PKHAs contain built-in routines to perform modular exponentiation and elliptic curve computations, as well as ordinary integer modulo arithmetic.

Data Encryption Standard Accelerators (DESA)

Each of the six **ZPCI.3910** DESAs support DES and Triple-DES in both ECB and CBC modes. In Triple-DES mode, these units support two key (K1, K2, K1) or three key (K1, K2, K3) processes.

Message Digest Hardware Accelerator (MDHA)

Each of the three **ZPCI.3910** MDHAs compute hash data using MD4 (128 bit), MD5 (128 bit) or SHA-1 (160 bit) algorithms. The MDHA also supports HMAC computations.

RC4 Compatible Stream Cipher Module (AFHA)

The **ZPCI.3910** AFHA module computes RC4 compatible stream type bulk data encryption with a 40 to 128-bit key

ZPCI.3910 Security Processor PCI Card

The **ZPCI.3910** implements a Motorola MPC190
Security Processor on a standard 3.3V 64-bit PCI card.

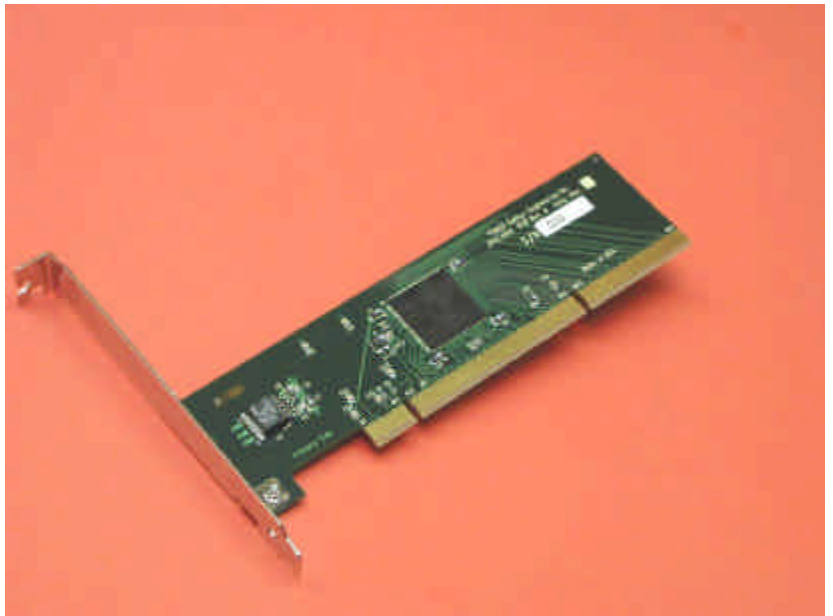## Compliance

PCI Local Bus Specification, R2.2

Specifications

3.3V 66 MHz, 64-bit PCI Interface
Bus Width: 64 or 32 bits*
PCI clock: 66 or 33 MHz**
Signaling levels: 3.3V
Slot power: 2W maximum

Input Power Requirements (typical 33 MHz)
+3.3V: 500 mA
+5.0V: 0 mA

Mechanical Dimensions
(excluding bracket):
1.8 in (45 mm) x 6.4 in (163 mm)
Maximum component height: 0.25 in (6 mm)

On-board Connectors
Standard 3.3V 64-bit PCI gold-plated edge connector

Warranty
One year limited warranty.

Ordering Information
Order number
ZPCI.3910   Security Processor PCI Card

* Automatic 32/64 bit detection of PCI bus width per
PCI specification rev 2.2
** Automatic 66/33 MHz detection of PCI bus speed
per PCI specification rev 2.2