

# ZPCI.3911

## MPC184 Security Processor PCI Card

**Security Processor optimized for IPsec, IKE, WTLS/WAP, SSL/TLS, 802.11i**

**5V/3.3V 33/66 MHz 32-bit PCI Interface**

**Rev 2.2 compliant PCI Bridge—usable in virtually any PCI slot**

**High-performance Bus-master Design**

- **Public Key Execution Unit**
  - Modular arithmetic and exponentiation with up to 2048-bit field size supports RSA and Diffie-Hellman
  - Elliptic curve operations with up to 511-bit field size support  $F_p$  and  $F_{2^m}$
- **Data Encryption Standard Execution Unit**
  - DES in ECB or CBC modes
  - 3DES in two key (K1, K2, K1) or three key (K1, K2, K3) ECB/CBC modes
- **Advanced Encryption Standard Execution Unit**
  - Rijndael symmetric key cipher
  - Support for ECB, CBC and counter modes
- **ARC Four Execution Unit**
  - RC4 compatible stream cipher with a 40 to 128-bit key
- **Message Digest Execution Unit**
  - MD5 (128-bit)
  - SHA-1 (160-bit)
  - SHA-2 (256-bit)
  - HMAC with any algorithm
- Random number generator
- 4 Crypto-channels, each with multi-command descriptor chain support
- PCI rev 2.2 compliant master/slave
- 5V/3.3V Low-power design (2W typical)
- On-board 1.5V regulator
- Software and development support



The **ZPCI.3911** MPC184 Security Processor PCI card from Zephyr Engineering, Inc is a high-performance encryption/decryption engine on a universal (5V/3.3V) 32-bit 66 MHz PCI card.

### High Performance

The **ZPCI.3911** MPC184 Security Processor PCI card is capable of performing 3DES encryption/decryption at rates of up to 144 Mbps and MD5 authentication at 176 Mbps.

### PCI Form Factor Gives You System Flexibility

You can plug the **ZPCI.3911** into any PCI slot. Install it in your PC along with a standard PCI ethernet card and you have a complete security processor system.

### Public Key Execution Unit (PKEU)

The **ZPCI.3911** PKEU contains built-in routines to perform modular exponentiation and elliptic curve computations, as well as ordinary integer modulo arithmetic.

### Data Encryption Standard Execution Unit (DEU)

The **ZPCI.3911** DEU supports 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 Execution Unit (MDEU)

The **ZPCI.3911** MDEU computes hash data using MD5 (128 bit), SHA-1 (160 bit) or SHA-2 (256 bit) algorithms. The MDEU also supports HMAC computations.

### ARC Four Execution Unit (AFEU)

The **ZPCI.3911** AFEU module computes RC4 compatible stream type bulk data encryption with a 40 to 128-bit key.



Visit us at [WWW.ZPCI.COM](http://WWW.ZPCI.COM)

ZEPHYR ENGINEERING, INC. 1620 WEST FOUNTAINHEAD PKWY, SUITE 320, TEMPE, AZ 85282-1876 (480)736-8714

## **ZPCI.3911 MPC184 Security Processor PCI Card**

The **ZPCI.3911** implements a Motorola MPC184 Security Processor on a universal (5V or 3.3V) 32-bit PCI card.

### **Compliance**

PCI Local Bus Specification, R2.2

### **Specifications**

#### **5V/3.3V 66 MHz, 32-bit PCI Interface**

Bus Width: 32 bits  
PCI clock: 66 or 33 MHz\*  
Signaling levels: 5V or 3.3V  
Slot power: 2W maximum



#### **Input Power Requirements (typical 33 MHz)**

+3.3V: 300 mA  
+5.0V: TBD mA

#### **Mechanical Dimensions**

(excluding bracket):  
2.75 in (69.8 mm) x 4.8 in (122.5 mm)  
Maximum component height: 0.25 in (6 mm)

#### **On-board Connectors**

Universal (5V/3.3V) 32-bit PCI gold-plated edge connector

### **Warranty**

One year limited warranty.

### **Ordering Information**

Order number  
ZPCI.3911 MPC184 Security Processor PCI Card

\* Automatic 66/33 MHz detection of PCI bus speed per PCI specification rev 2.2



Visit us at [WWW.ZPCI.COM](http://WWW.ZPCI.COM)

ZEPHYR ENGINEERING, INC. 1620 WEST FOUNTAINHEAD PKWY, SUITE 320, TEMPE, AZ 85282-1876 (480)736-8714

Rev 030728