ZPCI.3901

MPC184 Security Processor PMC Module

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

IEEE 1386 32-bit PCI Mezzanine Card

High-performance Bus-master Design

33/66 MHz 32 bit PCI Interface

PCI rev 2.2 compliant

- 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 supports F_p and F_2m
- 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
  - Rinjdael 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
- 3.3V Low-power design (1W typical)
- On-board 1.5V regulator
- Software and development support

The **ZPCI.3901** MPC184 Security Processor PMC module from Zephyr Engineering, Inc is a high-performance encryption/decryption engine on a 32-bit 66 MHz PMC form-factor card.

High Performance

The **ZPCI.3901** MPC184 Security Processor PMC module is capable of performing 3DES encryption/decryption at rates of up to 144 Mbps and MD5 authentication at 176 Mbps.

PMC Form Factor Gives You System Flexibility

You can drop the **ZPCI.3901** into any PMC slot. Add it to the PMC slot on your CPU card or install it on an SBC (such as Zephyr's **ZPC.1900** Security Processor Development Platform), VME, cPCI, PCI or standalone carrier board (such as Zephyr's **ZPCI.2900** Quad PMC Carrier).

Public Key Execution Unit (PKEU)

The **ZPCI.3901** 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.3901** 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.3901** 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.3901** AFEU module computes RC4 compatible stream type bulk data encryption with a 40 to 128-bit key.

Visit us at WWW.ZPCI.COM

Zephyr Engineering, Inc. 1620 West Fountainhead Pkwy, Suite 320, Tempe, AZ 85282-1876 (480)736-8714

ZPCI.3901 Security Processor PMC Module

The **ZPCI.3901** implements a Motorola MPC184 Security Processor on a single IEEE1386.1 PMC card.

Compliance

IEEE P1386.1 PMC Draft Specification
PCI Local Bus Specification, R2.2

Specifications

IEEE P1386.1 32-bit PMC Interface

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

Input Power Requirements (typical 33 MHz)

+3.3V:	300 mA
+5.0V:	0 mA

Mechanical Dimensions

Standard IEEE P1386.1 PMC form factor:
2.5 in (65 mm) x 6.0 in (150 mm)
Standard IEEE P1386.1 PMC height:
0.50 in (13 mm)

On-board Connectors

Two 64-pin connectors for 32 bit PMC: J1 and J2

Warranty

One year limited warranty.

Ordering Information

Order number

ZPCI.3901	Security Processor PMC Module
ZPC.1900	Security Processor Development Platform
ZPCI.2900	Quad PMC Carrier

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