ZPCI.3900

MPC190 Security Processor PMC Module

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

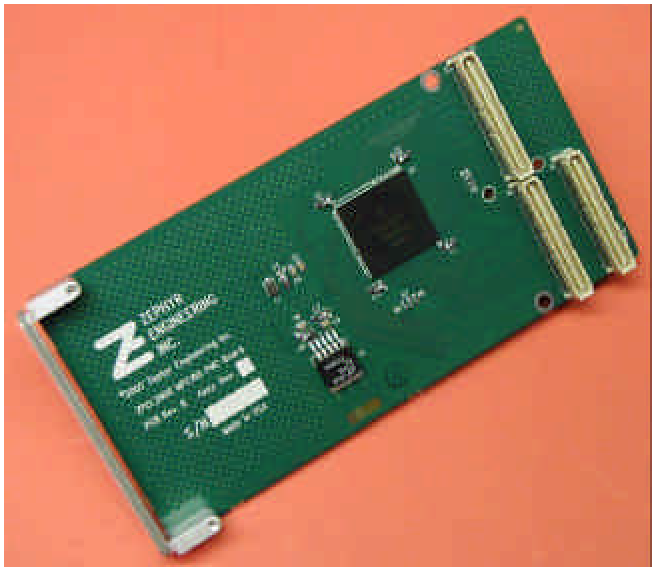
IEEE 1386 64-bit PCI Mezzanine Card

High-performance Bus-master Design

33/66 MHz 32/64 bit PCI Interface

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.3900** MPC190 Security Processor PMC module from Zephyr Engineering, Inc is a high-performance encryption/decryption engine on a 64-bit 66 MHz PMC form-factor card.

High Performance

The **ZPCI.3900** MPC190 Security Processor PMC module is capable of performing 3DES encryption/decryption at rates of up to 0.68 Gbps and MD5 authentication at 0.97 Gbps.

PMC Form Factor Gives You System Flexibility

You can drop the **ZPCI.3900** into any PMC slot. Add it to the PMC slot on your CPU card or install it on an SBC, VME, cPCI, PCI or standalone carrier board such as Zephyr's **ZPCI.2900** Quad PMC Carrier.

Public Key Hardware Accelerators (PKHA)

Each of the six **ZPCI.3900** 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.3900** 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.3900** 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)

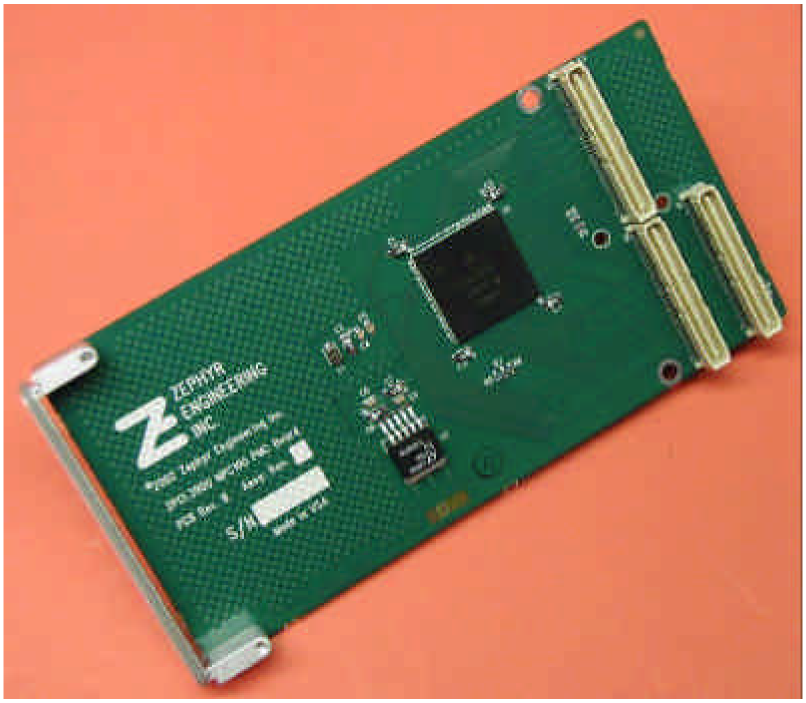
The **ZPCI.3900** AFHA module computes RC4 compatible stream type bulk data encryption with a 40 to 128-bit key

Visit us at WWW.ZPCI.COM

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

ZPCI.3900 Security Processor PMC Module

The **ZPCI.3900** implements a Motorola MPC190 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 64-bit PMC 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:	TBD 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

Three 64-pin connectors for 64 bit PMC: J1, J2 and J3

Warranty

One year limited warranty.

Ordering Information

Order number

ZPCI.3900	Security Processor PMC Module
ZPCI.2900	Quad PMC Carrier

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