

# Hifn-class Security for Space and Power Constrained Applications

## SentryXL™ ASPs – 7964/7965/7966



### The industry's smallest and lowest power processors for encryption, compression, and hashing

You've heard how all the most powerful Internet Routers, switches and communication infrastructure equipment are powered with Hifn's Applied Services Processors (ASPs) – now that same performance is available for space and power constrained applications such as environmentally-hardened wireless base stations, wireless access points, multi-function networked printers, and portable communication devices. The SentryXL family delivers the strongest industry-standard encryption, compression, and hashing available in its class in one quarter the size of its predecessor, and with the lowest power consumption. Customers no longer have to settle for anything less than full business-class connectivity, and suppliers can reap the benefits of offering premium security hardware acceleration for little more than the cost of software implementations. Easy to embed, and delivering the best performance per square mm and per mw of power, the SentryXL family consists of the 7964, 7965, and 7966 devices.

### Full Security Protocol Support

Power and space starved devices no longer have to compromise on security features. The SentryXL family offers security engines that accelerate a variety of IPsec and SSL/TLS protocols including DES, Triple DES, AES (128, 192, and 256-bit, with counter mode support), MD5, and SHA-1. Also included is a true Random Number Generation, and Public Key processor for accelerating IKE and SSL/TLS handshaking.

### Dual Host Bus Interface

The SentryXL devices can be configured to either interface with Motorola MPC860 or MPC8260 bus, or a PCI2.2 bus without any glue logic.

### Count on Hifn's Experience and Expertise

With comprehensive development software programs in place, Hifn can dramatically improve time-to-market while reducing development costs. The SentryXL family of ASPs is pin and software compatible providing easy to embed solutions for multiple price/performance products based on a single system design. Additionally the SentryXL software API is completely backwards compatible with the previous and proven 7954/55/56, 7902, and 7951 API toolkits.

#### COMPRESSION

- LZS
- MPPC

#### PUBLIC KEY

- RSA, DH, DSA
- True Random Number Generator

#### ENCRYPTION

- AES (128, 192, 256-bit and counter mode)
- DES
- 3DES
- ARC4\*

#### AUTHENTICATION

- SHA-1
- MD5

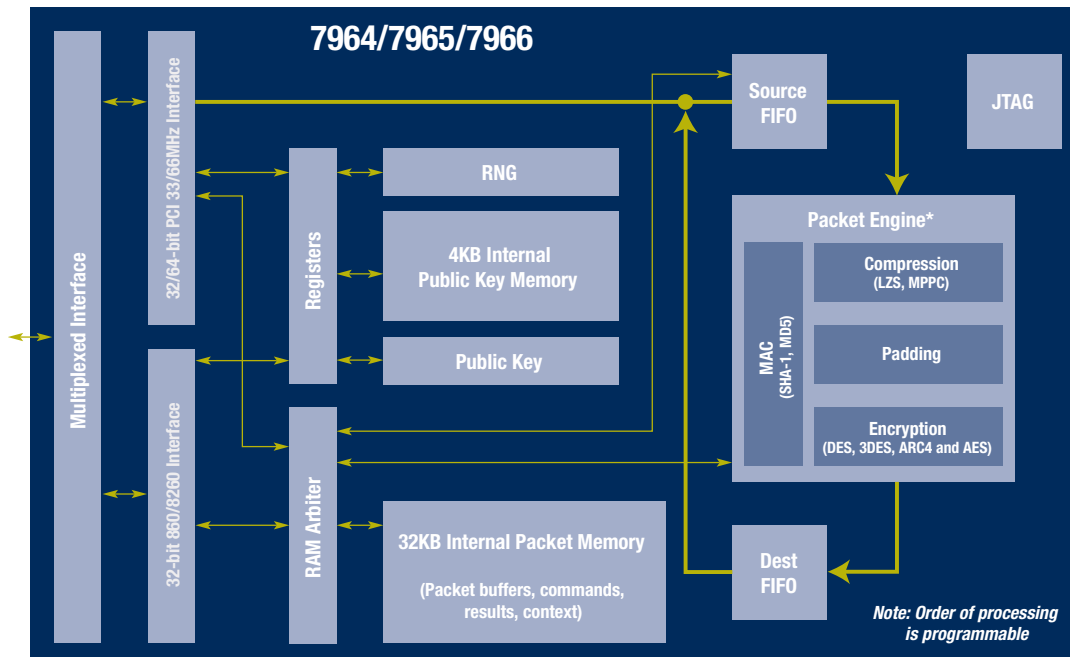
#### MULTIPLEXED INTERFACE BUS

- MPC8260
- MPC850/860
- PCI rev 2.2

#### TUNNELING PROTOCOLS

- IPsec
- L2TP
- PPTP

\*Algorithm completely compatible with RSA's RC4.™



7964, 7965 and 7966 Internal Diagram

Accelerates Layer 3 and Layer 2 protocols

### IPSEC (LAYER 3)

- RFC 2401 – IP Security Architecture
- RFC 2393 – IP Payload Compression
- RFC 2406 – IP Encryption
- RFC 2402 – IP Authentication
- RFC 2395 – IP Compression/LZS
- RFC 2405 – DES-CBC Cipher Algorithm
- RFC 2403 – HMAC-MD5
- RFC 2404 – HMAC-SHA-1

### PPP (LAYER 2)

- RFC 1962 – Compression Control Protocol
- RFC 1967 – PPP LZS-DCP Compression
- RFC 1974 – PPP LZS Compression
- RFC 2118 – Microsoft Point-to-Point Compression (MPPC)

### PPTP

- RFC3078 - MPPE

\* Performance measured using a typical system configuration

750 University Avenue  
Los Gatos, CA 95032  
408.399.3500 tel  
408.399.3501 fax  
info@hifn.com

[www.hifn.com](http://www.hifn.com)

## Features and Benefits

### High Performance\*

- **7964:** AES/SHA1—162 Mbps
- **7965:** AES/SHA1—312 Mbps
- **7966:** AES/SHA1—554 Mbps
- Compression engine increases effective throughput
- Supports 256 simultaneous sessions on chip, and unlimited sessions in host memory

### Low Power Consumption

- **7964:** 0.3W typical
- **7965:** 0.6W typical
- **7966:** 0.8W typical

### Accelerates All Major Security and Compression Protocols

- IPsec in transport and tunnel modes: AH, ESP, AH+ESP (including dual MAC), with or without IPPCP (IP compression)
- Stateful and stateless PPTP (MPPE and MPPC) processing
- Stateful PPP compression processing
- 128/192/256-bit AES, DES, 3DES, and ARC4 encryption
- SHA-1 and MD5 hashing and authentication
- LZS and MPPC compression
- Public-Key support accelerates RSA, DSA, SSL, IKE, and Diffie-Hellmann
- Supports up to 3,072-bit modular arithmetic and exponentiation
- True Hardware Random Number Generator

### Efficient Multiple Bus Architecture

- Bus-mastering 32 or 64-bit PCI rev 2.2 interface at 33 or 66MHz
- Direct Interface to MPC860 or MPC8260-bus interface

### Low Host Overhead

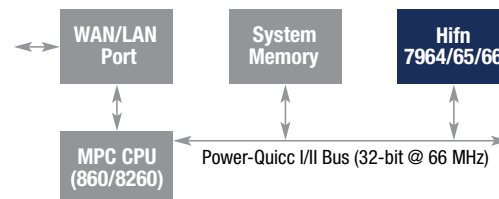
- Session contexts may be stored in on-chip private memory
- Descriptor-based DMA engine (supports data scatter/gather)
- On-chip memory used to buffer control data packets in PowerQuicc modes
  - Enables reduced processing latency when used for packet buffering
- Built-in ROM or optional low-cost external EEPROM provides maximum configuration flexibility

### Software Support

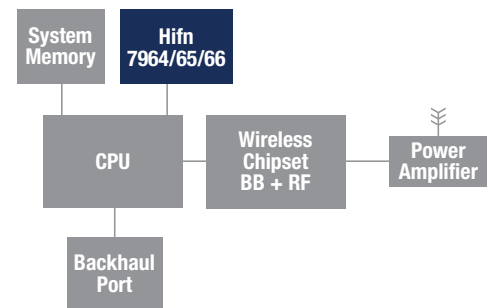
- Supported by the Hifn 7964/65/66 Development Kit (HDK) API
- API supports the full feature set of Hifn 7964/65/66 products
- API works with a wide range of host architectures

### Other Features

- Supports programmable Muting Table Memory for MAC operations
- Supports low-cost implementations with 144-pin PFBGA
- On-chip PLL enables flexible low-cost external clock input
- JTAG support
- Reference hardware design
- 1.5V core with 3.3V I/O



Example System Concept (PowerQuicc I and II Bus Mode)



Wireless Base Station

## Ordering Information

Part Number	Core/PK	Package
7964PP6/2-G	33/66 MHz	144-pin PFBGA
7965PP6/2-G	66/133 MHz	144-pin PFBGA
7966PP6/2-G	133/133 MHz	144-pin PFBGA

## Documentation

- Device Specification
- Software Getting Started Guide
- Software Users Guide
- Software Diagnostics User Guide
- Design and Performance App Notes