# Hifn HIPP III
Storage Security Processor
4350

## Protocols
- IPsec ESP
- Tunnel or Transport Mode
- Supports L2TP Security
- ESP/UDP for NAT

## Encryption
- AES (128 and 256-bit)
- DES
- 3DES

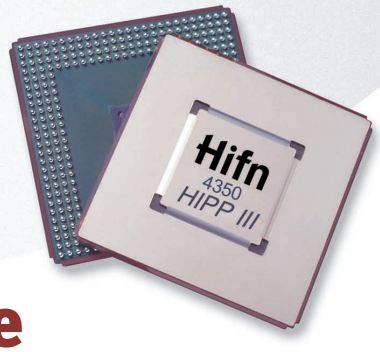
## Authentication
- SHA-1
- MD5
- AES-XCBC-MAC

## Interface Bus
- 4x GMII or TBI

## On-Chip IKE
- Optional ICSA-compliant IKE running on-board
- Supports Main Mode & Quick Mode
- Pre-shared Key or RSA certificate authentication
- Supports iSCSI initiation of IKE session setup and teardown

Hifn
Intelligent Secure Networking

# Preserve Data Security and Integrity for Both iSCSI and FCIP Hardware




## The HIPP III 4350 Storage Security Processor efficiently addresses your needs for a standards compliant 2-port gigabit Ethernet solution

The Hifn™ HIPP III 4350 Storage Security Processor is the first security processor designed for the specific requirements of IP Storage applications. The 4350 offers a complete IPSec data path solution optimized for IP Storage based systems, combining inbound and outbound policy processing, SA lookup, SA context handling, and packet formatting – all within a single chip. Hifn's 4350 delivers industry-leading cryptographic functionality, supporting the DES/3DES-CBC, AES-CBC, AES-CTR, MD5, SHA-1 and AES-XCBC-MAC algorithms. Hifn also provides complete software support, including an on-board iSCSI-compliant IPSec software stack, offering an embedded HTML manager application.

The HIPP III 4350 employs Hifn's FlowThrough™ Security Architecture to deliver two channels of full-duplex Gigabit Ethernet encrypted throughput in iSCSI (Internet Small Computer System Interface), FCIP (Fibre Channel over IP) and other IP-based storage networking systems. The high-speed HIPP III 4350 is optimized for use in server host bus adapters, FCIP bridges, storage routers, and storage arrays.

### Hifn's FlowThrough Security Architecture

Hifn's FlowThrough Security Architecture is the cornerstone of a new family of solutions that vitally change the way security is built into the network.

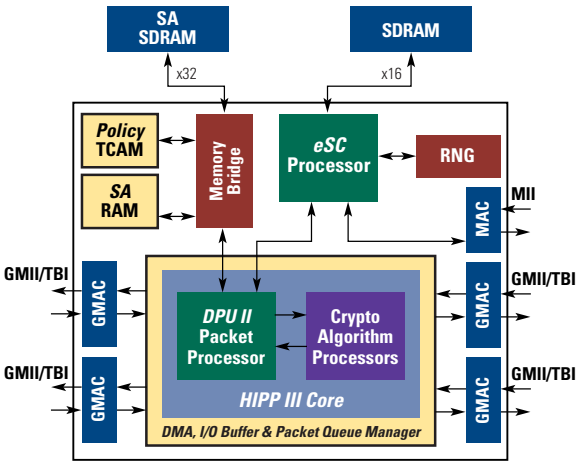
The new architecture enables security processors that sit directly in the data path, eliminating the inefficiencies of existing "look-aside" security designs.

Fundamental to the new FlowThrough architecture is the acceleration of the entire data path of the IPSec protocol, which previously represented a heavy processing load on the Storage Processor or other processing elements in the system. The new architecture incorporates packet processing, link layer processing for Ethernet, security association handling, and IPSec encryption/ authentication functions into silicon-based products. Hifn's FlowThrough Security Architecture enables high-performance, cost-effective security processors that provide wire-speed performance for encrypted traffic in IP Storage and high-performance network equipment.

### Easy Integration

The HIPP III 4350 uses industry-standard GMII/TBI interfaces, supported by numerous GigE TOE (TCP Offload Engine) and Storage Processor vendors. It is typically interfaced between the GMII ports on a GigE TOE or Storage Processor and the Ethernet PHY. The 4350 supports two full-duplex Gigabit Ethernet ports.

The control interface to the 4350 is achieved using in-band Ethernet frames. An additional 100Mbps Ethernet MII port allows an optional out-of-band control port, or it may be used to establish an inter-chip link for multi-chip designs. The chip includes two standard PC-133 SDRAM interfaces. One is used for program and data storage for the on-board embedded Session Control (eSC) processor. (In designs that don't require on-chip IKE, this RAM can be omitted.) The second SDRAM interface is used to store Security Associations (SAs) when many hundreds or thousands of secure tunnels are required. These standard interfaces allow integration into a variety of systems.




*HIPP III 4350 Block Diagram*

# Hifn HIPP III

Storage Security Processor

4350

## Supports Layer 3 and Layer 2 protocols.

### Ethernet (Layer 2)

Ethernet DIX

IEEE 802.3 10Base-T

IEEE 802.3u 100Base-TX

IEEE 802.3ab 1000Base-X

IEEE 802.3x Flow Control

IEEE 802.2 LLC

IEEE 802.1q VLAN

RFC1042 SNAP

Jumbo 9K frame support

### IPSec (Layer 3)

RFC 2401 – IP Security Architecture

RFC 2406 – IP Encryption

RFC 2405 – DES-CBC Cipher Algorithm

RFC 2403 – HMAC-MD5

RFC 2404 – HMAC-SHA-1

RFC 2409 - IKE

Hifn

Intelligent Secure Networking

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

# Features & Benefits

### Single-chip, low-cost solution

- 4Gbps IPSec processing (Full Duplex Dual GigEthernet)
- 1M Packets Per Second, back-to-back SA variation
- Minimal part count: Inexpensive PC-133 SDRAMs support on-chip IKE and/or optional local SA storage

### FlowThrough™ security processing

- In-line IPSec protocol and algorithm processing
- Streamlined & optimized for storage security
- On-chip IKE processing (optional)
- Complete IPSec/IKE processing enables easiest IPSec system implementation

### Optimized for site-to-site tunnels

- 200 SAs supported on-chip
- Up to 16,000 SAs with external PC-133 SDRAM
- 256 on-chip policy entries

### Full IPSec Compliant Functionality

- IPSec ESP in tunnel and transport modes
- AES (CBC & CTR), DES/3DES, SHA-1, MD5, AES-XCBC-MAC

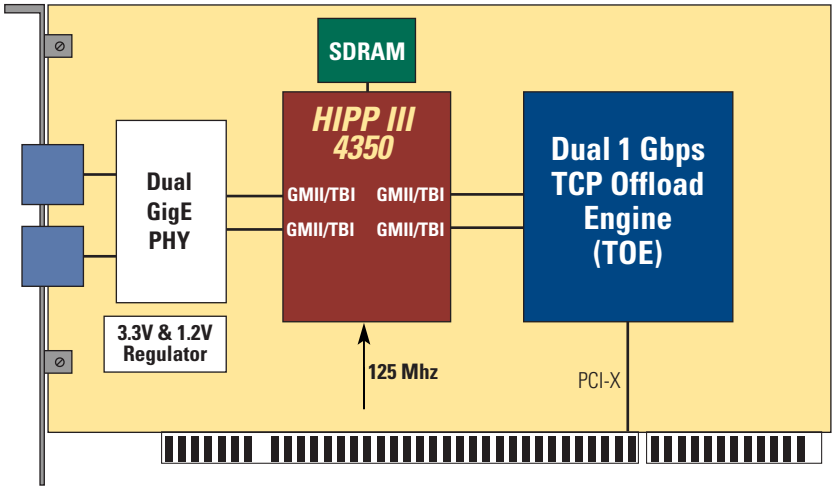
### Specifications

- 13µ process, 324 LBGA (19mm square)
- <1.75W Power consumption

# Applications

### IP Storage

- Host Bus Adaptors (HBA's)
- Target Bus Adaptors (TBA's)
- SAN Switches
- Storage Servers




***Example Host Bus Adaptor with HIPP III 4350***

## Hifn Product Selection Guide

| Hifn Products | PCI | Streaming Bus | LZS MPPC | 3-DES AES | SHA MD5 | RSA DSA | 1k-bit RSA SSL signatures set-ups per second | IKE main-mode tunnels per second | Hardware support for public keys up to | Hifn Intelligent Packet Processing | Package |
|---|---|---|---|---|---|---|---|---|---|---|---|
| HIPP I 7815 | ■ | ■ | ■ | ■ | ■ | ■ | 120 | 85 | 2K bits | ■ | 480-pin BGA |
| HIPP I 7855 | ■ | ■ | ■ | ■ | ■ | ■ | 241 | 150 | 2K bits | ■ | 480-pin BGA |
| HIPP II 8065 | ■ | ■ | ■ | ■ | ■ | ■ | 2000 | 1750 | 3K bits | ■ | 576-pin TBGA |
| HIPP II 8165 | ■ | ■ | ■ | ■ | ■ | ■ | 4500 | 1750 | 3K bits | ■ | 576-pin TBGA |
| HIPP II 8154 | ■ | ■ | ■ | ■ | ■ | ■ | 906 | 1000 | 3K bits | ■ | 576-pin TBGA |
| HIPP III 8300 | | ■ | | ■ | ■ | ■ | 250 | 90 | 4K bits | ■ | 324-pin LBGA |
| HIPP III 8350 | | ■ | | ■ | ■ | ■ | 400 | 150 | 4K bits | ■ | 324-pin LBGA |
| HIPP III 4300 | | ■ | | ■ | ■ | ■ | 10 | 5 | 4K bits | ■ | 324-pin LBGA |
| HIPP III 4350 | | ■ | | ■ | ■ | ■ | 300 | 75 | 4K bits | ■ | 324-pin LBGA |

## Ordering Information

| Part Number | Speed | Package |
|---|---|---|
| 4350 | 200 Mhz | 324 LBGA |

**Documentation:**

Datasheet
User's Manual
Programmers Reference Guide
Performance Application Note
Reference Hardware Document