Hifn

# HIPP II

Security Processor

8154

## Compression

- LZS
- MPPC

## Encryption

- AES
- DES
- 3DES
- ARC4*

## Authentication

- SHA-1
- MD5

## Public Key

- RSA, DH, DSA
- Hardware random number generator

Hifn

Intelligent Secure Networking

# HIPP II– World's first gigabit security processor with onboard public key

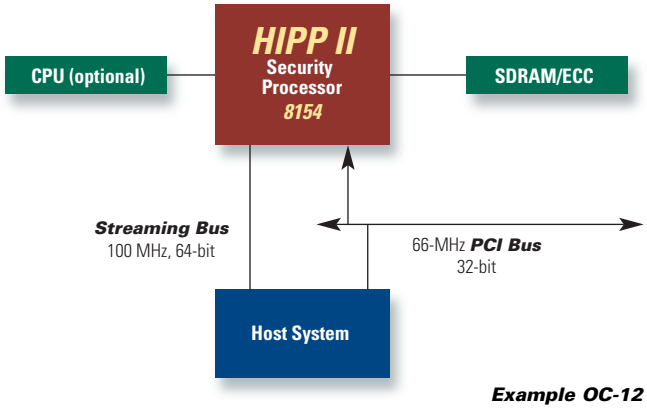

## Full-duplex OC-12 to full-duplex OC-48, integrated public key, 3DES and AES, compression – the HIPP II model 8154 breaks the performance barrier with a single chip

The HIPP II model 8154 security processor recognizes and operates on packets that contain multiple protocols- such as IPSec and SSL- virtually eliminating the computational overhead of host processors in routers and other networking equipment, all at full-duplex gigabit speeds. Plus, connect two 8154s with the streaming interface and you get 3,000 IKE Quick Mode connections per second at full duplex OC-48 data rates, even on small packets, providing your customers the fastest and most complete security solution available in the market today.

Hifn™ is the first company to implement packet processing as part of the security acceleration solution, thereby speeding up the entire process of compression, encryption, authentication, public key and random number generation. Other security solutions tend to concentrate on performing the various IPSec algorithms, leaving CPUs or network processors to deal with the complex header and trailer processing, packet fragmentation, and other packet processing issues. With Hifn Intelligent Packet Processing (HIPP) at your side, you will have the benefit of increased system performance.

## Common processor architecture, plus Hifn's unmatched design experience, means faster time to market and higher reliability

Adopt the Hifn architecture and you'll be able to concentrate your design efforts on creating the best possible network access products, because the security part of your design is extensible and scalable, with a rock-solid software wrap. It includes a HIPP Software Developer's Kit (SDK) or Hifn's Security Platform, HSP, which also clears the way towards FIPS 140-1 level 3 compliance. You can take your pick of solutions from IPSec T3 to multi-gigabit data rates, or SSL e-commerce security processors. Either way, you can choose a starting point with the knowledge that the next Hifn chip will fit in your design with a minimum of effort. Hifn engineers have helped design security into the world's most highly regarded routing and networking equipment, made by companies such as Cisco, Nortel, Lucent, and many others.




*Example OC-12 System Block Diagr*

# Hifn HIPP II Security Processor 8154

**Supports 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

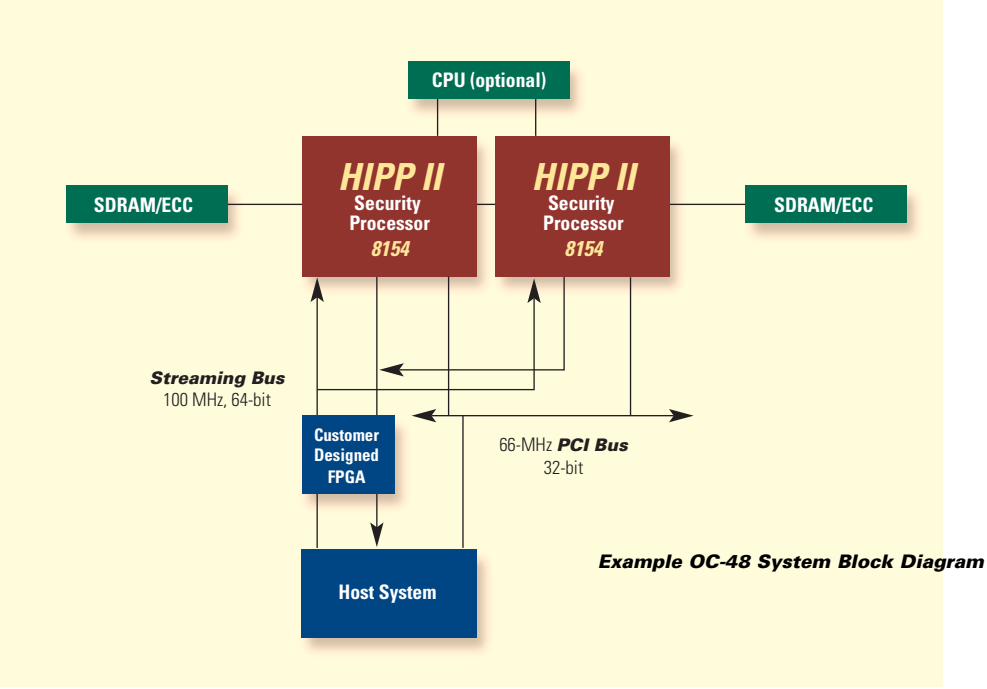
RFC 2118 – Microsoft Point-to-Point Compression (MPPC)


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

- HIPP architecture results in minimal host CPU interaction and maximum system performance
  - Single pass header & trailer processing, compression, encryption and authentication
  - On-chip processing for mutable fields, anti-replay, stateful sequence number checking and header checksum modification
- 2,048 Mbps IPSec (3DES/SHA-1 or AES/SHA-1)
- 1,500 IKE Quick Mode connections per second
- Support for up to 3,072-bit public keys natively
- LZS and MPPC compression engines run at up to 3.2 Gbps and increase the effective data rate throughput of the 8154 when enabled
- Stateful packet processing and support of ARC4* algorithm maximize PPTP performance
- High speed 32 or 64-bit/66MHz PCI or Streaming Bus interface
- HSP Architecture enables FIPS 140-1 level 3 compliance
- Over 500K simultaneous sessions supported
- HSP or SDK software shortens development cycle
- 576 TBGA package




*Example OC-48 System Block Diagram*

## Hifn Product Selection Guide

| Hifn Products | Delivered Mode | PCI | LZS | MPPC | DES 3-DES ARC4* | SHA MD5 | RSA DSA | AES |
|---|---|---|---|---|---|---|---|---|
| 6500 | Silicon | ■ | | | | | ■ | |
| 7851 | Silicon | ■ | ■ | ■ | ■ | ■ | | |
| HIPP | Silicon | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| 7901 | Silicon | | ■ | ■ | ■ | ■ | ■ | |
| 7902 | Silicon | | ■ | ■ | ■ | ■ | ■ | |
| 7951 | Silicon | ■ | ■ | ■ | ■ | ■ | ■ | |
| HIPP II | Silicon | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| LZS-221 | Software | | ■ | | | | | |
| MPPC | Software | | | ■ | | | | |
| HSP | Software | | ■ | ■ | ■ | ■ | ■ | ■ |

## HIPP II Ordering Information

| Part Number | Package |
|---|---|
| 8154-PB5 | 576-pin TBGA |

**Documentation:**
Datasheet
Device Specification
Programmer's Reference Guide
DPU Programs Reference Manual
Performance Application Note
Reference Hardware Document
Power Consumption Apps Note

*Algorithm completely compatible with RSA's RC4.™