

# Hifn 7951

Security Processor

## Compression

- LZS
- MPPC

## Encryption

- DES
- Triple-DES
- ARC4\*

## Authentication

- SHA-1
- MD5

## Public Key

- RSA, DH
- Hardware random number generator

## Broadband Security Bargain Now with PCI Bus



### New Value-Priced Chip Powers High-Speed Small Office VPNs

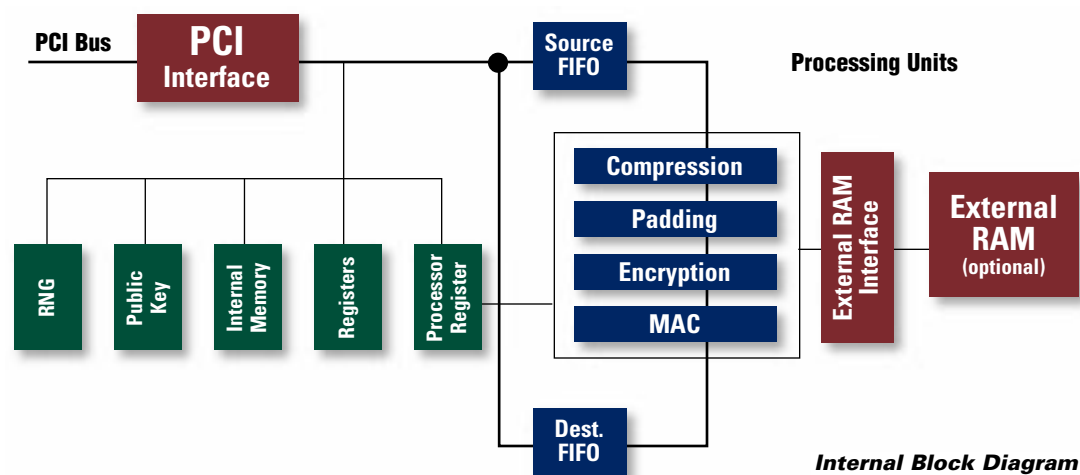
DSL, cable modems and other broadband applications demand hardware security acceleration—as much as 50-100 MIPS for IPSec processing. Now you can design in the strongest virtual private network security without sacrificing performance or spending big bucks.

### Soups up 3-DES and Public Key Processing

The 7951 crunches through compression, encryption and authentication algorithms at speeds that leave general-purpose CPUs in the dust. And, you get a true random number generator and Public Key acceleration, all on the same affordable all-purpose chip.

### Saves Money, Time and Board Space

At less than \$25,\* our new 7951 security processor fits within your budget and on your motherboard. Plus, the feature-packed 7951's PCI Bus interface reduces chip count and design time.



# Hifn 7951 Security Processor

**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

- Single chip multi-algorithm acceleration (LZS, 3-DES, SHA, Public Key & more)
- On-board IKE processor (2048-bit key lengths) and true random number generator
- Concurrent symmetric and Public Key processing
- Compression (LZS and MPPC)
- 32 Mbps processing
- Multi-protocol support: IPSec, IPPCP (IPCOMP), PPTP, L2TP, PPP and IKE
- PCI Bus interface

## Benefits

- Off-loads compute-intensive work from CPU
- Delivers top security protection and breaks performance bottlenecks
- Non-stop performance
- Improves speed
- VPN at full broadband speed
- Interoperates with all major vendor's equipment
- Industry standard Bus

## Tools

- Software API for faster time to market
- PCI evaluation board

## Broadband Performance Requirements

WAN Link	WAN Speed (Mbps)	7951 Throughput (Mbps)
ISDN	.128	32
DSL	.128	32
T1	1.5	32
E1	2.0	32
ADSL	8.0	32

## Hifn Product Selection Guide

	Hifn Products	Delivered Mode	PCI	LZS	MPPC	DES 3-DES ARC4*	SHA MD5	RSA DSA
Encryption Products	6500	Silicon	■					■
	7711	Silicon		■	■	■	■	
	7751	Silicon	■	■	■	■	■	
	7811	Silicon	■	■	■	■	■	
	7851	Silicon	■	■	■	■	■	
	7901	Silicon		■	■	■	■	■
	7951	Silicon	■	■	■	■	■	■
	IPSECure**	Software		■		■	■	■

\*\*IPSECure does not include ARC4\*

	Hifn Products	Delivered Mode	PCI	LZS	MPPC	ALDC
Compression Products	9600	Silicon		■		
	9602	Silicon				■
	9603	Silicon		■		
	9610	Silicon		■		
	9710	Silicon		■		
	9711	Silicon		■	■	
	9751	Silicon	■	■	■	
	LZS-221	Software		■		
	MPPC	Software			■	

## Ordering Information

Part Number	Package
7951 PT6	144-pin TQFP



©2000 by Hi/fn, Inc. This product must be exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law prohibited. Hi/fn is a trademark of Hi/fn, Inc. Hi/fn and LZS are registered trademarks of Hi/fn, Inc. All other trademarks are the property of their respective owners.  
\*Algorithm completely compatible with RSA's RC4™.