World Class Security Performance…for Less

APPLIED SERVICES PROCESSOR – 7855

HIFN
PROTECT · SECURE · ASSURE

The 7855 gives designers an increase in system performance, without digging deep into their pocketbook

The 7855 Applied Services Processor (ASP) is a highly integrated cryptographic processor capable of performing DES, 3DES, ARC4, AES (128, 192, 256-bit) with all modes of operation (ECB, CBC and Counter Mode) at full-duplex T3 to full-duplex OC12 speeds.

The 7855's on-board DPU (Dynamic Protocol Unit) processes protocols based on the available hardware algorithms. Support includes IPsec, SSL, IPPCP, PPTP, IPComp and IPv4/IPv6. Packets are passed to the engine via a 64-bit/66MHz PCI bus interface.

When Hifn's first security processors were announced in November 2000, the concept of full-packet processing on-chip was new to the security processor market. Now, with so much network traffic requiring some level of security these days, the ability to support line-speed encryption and decryption has become a requirement. Hifn's line of ASPs have become the industry-proven way to reduce system latency and guarantee system performance.

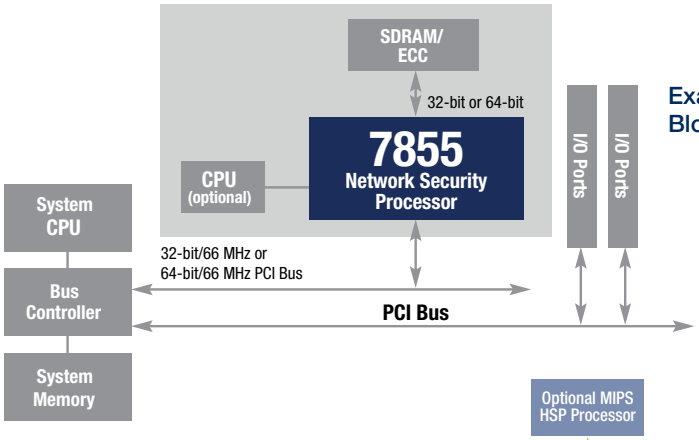
Easy Integration

Because the 7855 does so much of the heavy lifting, integration with a control processor, host system, or network processor is greatly simplified. Most operations can be treated as API calls, allowing the rest of the system to pay attention to other important tasks like policy enforcement and traffic management. The simplified programming requirements also translate into much shorter development efforts.

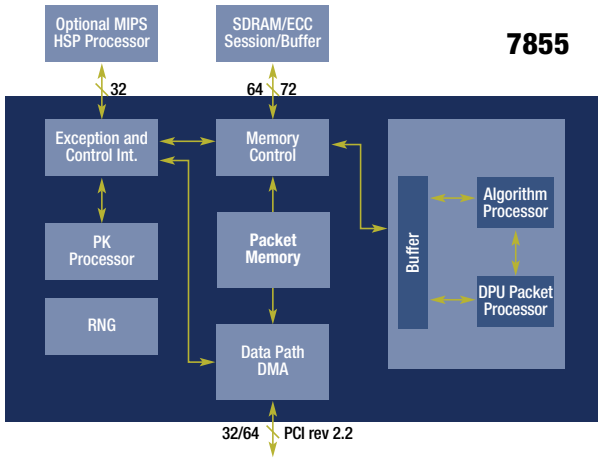
Easy Migration

With Hifn's common hardware and software architecture approach, manufacturers are able to update their products to different performance levels with a minimum of effort.

For years, Hifn's security expertise has helped customers design their security into an array of products; from DSL and cable solutions to the highly advanced multi-gigabit IP service switches. You can depend on Hifn as you design your next networking products.



Example System Block Diagram



Chip Architecture

COMPRESSION
- LZS
- MPPC

ENCRYPTION
- AES (128, 192, & 256-bit), ECB, CBC, and Counter modes
- 3DES/DES
- ARC4*

AUTHENTICATION
- SHA-1
- MD5
- HMAC-SHA1
- HMAC-MD5

PUBLIC KEY
- RSA, DH, DSA
- Random Number Generator

INTERFACE BUS
- PCI 64bit/66MHz

TUNNELING PROTOCOLS
- IPsec (ESP, AH, Transport, and Tunnel)
- IPComp (IPPCP)
- SSL/TLS
- IPv4
- IPv6

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

APPLIED SERVICES PROCESSOR – 7855

APPLICATIONS

- VPN Gateways
- Firewall Appliances
- Mid-range VPN Enabled Routers
- SSL - VPN Gateways
- Wireless Gateways
- VoIP Gateways
- SAN Gateways

Features and Benefits

Intelligent Packet Processing architecture results in minimal host CPU interaction and maximum system performance.

- On-chip header and trailer processing
- On-chip processing for mutable fields, anti-replay, stateful sequence number checking and header checksum modification
- Single-pass compression, encryption and authentication
- 677 Mbps IPsec (AES/SHA-1)
- Lower BOM cost – requires minimal peripheral components to give you a lower system cost
- 360 DH (1024-bit key) exchanges per second
- Support for wide-key AES (128, 192, and 256-bit) and AES counter mode
- LZS and MPPC compression engines run at up to 875Mbps and increase the effective data rate throughput when enabled
- LZS compression is ideal for wireless applications
- Stateful packet processing and support of ARC4* algorithm maximize SSL and PPTP performance
- High speed 64-bit/66MHz PCI
- 512K simultaneous sessions supported
- HSP or SDK software shortens development cycle
- HSP architecture enables FIPS 140-2 level 3 compliance
- 2.0W typical power consumption

Supported Protocols

Supports Layer 3 and Layer 2 protocols

IPsec (Layer 3)

- RFC 4301 – 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

SSL/TLS

- RFC 2246 – TLS
- RFC 3546 – TLS Extensions
- RFC 3943 – TLS Compression

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

Features at a Glance

Hifn Product	PCI	LZS MPPC	3-DES AES	SHA MD5	RSA DSA	AES/SHA1 Performance	DH (1024-bit key, 184-bit exponent) exchanges per second	Hardware support for public keys up to	Packet Processing On Chip	Power (typical)
7855	■	■	■	■	■	677 Mbps	360	2K bits	■	2.0W

Ordering Information

Part Number	Speed	Package
7855PP4	133MHz	480-pin BGA
7855PP6	133MHz	625-pin BGA
7855PP4-G	133MHz	480-pin BGA
7855PP6-G	133MHz	625-pin BGA

Documentation

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

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

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