Secure VoIP
Processors

Protocols
- SRTP/SRTCP
- IPsec – AH, ESP, Tunnel mode, Transport mode
- SSL / TLS

Symmetric Transforms
- AES – 128, 192, 256, ECB, CBC, CTR
- DES, 3DES
- ARC4

Authentication
- SHA-1, MD5
- PK Operations
- RSA
- Diffie-Hellman
- DSA

True Random Number Generator

Interface Bus
- 8170 – PCI-X 64-bit/133MHz
- 8170 POS-Phy level 3
- 7870 66 MHz 64bit PCI

Packaging
- 8170 576 PBGA
- 7870 625 PBGA
- RoHS compliant

Power Consumption
- 8170 - 4W
- 7870 – 2.6W

First Family of Security Processors Designed Specifically for VoIP

Hifn's Secure VoIP Processors are the industry's first family of security processors designed specifically to protect VoIP traffic. These processors offer state of the art, cryptographic protection against a wide range of threats to both the signaling and media streams of VoIP services. Multiple protocols, low latency, high connectivity and high throughput make these devices ideal for a wide range of VoIP network elements including Session Border Controllers, Media Gateways, Media Servers and Packet Switches.

There are two processors in the Secure VoIP product line; the 7870 processor offers an estimated 250K small packets per second throughput and can support up to 512 thousand concurrent sessions. The 8170 processor can handle an estimated 1 million small packets per second and 1 million concurrent sessions. Both processors offer public key (PK) cryptography acceleration and true hardware random number generators. Both processors can handle any mix of Secure RTP (SRTP), Secure RTP control protocol (SRTCP), IPsec, Secure Sockets layer (SSL) or Transport Layer Security (TLS). These processors also support the new Datagram TLS (DTLS) protocol.

VoIP security involves many protocols for both signaling and media. Hifn's Secure VoIP processors handle randomly intermixed protocols (SRTP, IPsec, SSL/TLS) so they can simultaneously protect all VoIP data streams. No prior allocation of processor resources to protocols is necessary.

The very low processing latency of Hifn Secure VoIP processors guarantees that adding cryptographic protection to a network element will not exceed the device's latency budget.

Hifn Secure VoIP Processors support large numbers of concurrent sessions as well as a fast context setup and teardown time, which allows very high density statistical multiplexing of calls. A single, low cost chip can provide security services for thousands of calls and thousands of call setups per second.

Hifn's Intelligent Packet Processing (HIPP) Software Development Kit (SDK) is provided with the family of Secure VoIP Processors. The SDK offers a high level device enablement API that makes integration of Secure VoIP Processors fast and simple. Open source drivers for Linux and BSD operating systems are also available. Reference boards are provided with the SDK so that system integration and software development can begin immediately.
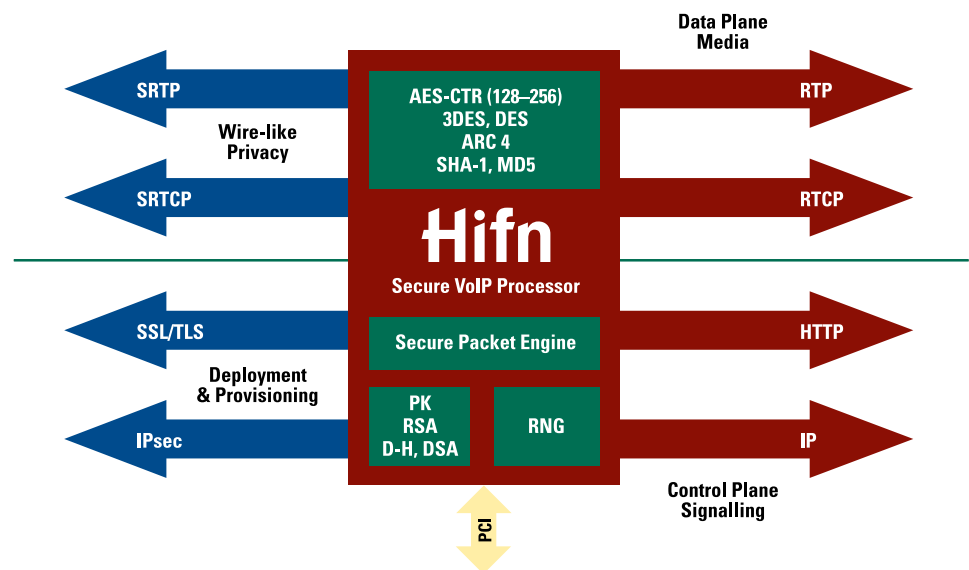
Secure VoIP Processor Services

Hifn
Intelligent Secure Networking

Hifn
Intelligent Secure Networking

8170 Secure VoIP Processor

The 8170 Secure VoIP Processor is Hifn's highest performance VoIP security product. The 8170 supports approximately 5,000 – 10,000 secure full duplex calls. With multi-gigabit throughput the 8170 is suitable for high capacity SBCs, Media Gateways and Class 5 Packet switches.

The 8170 interfaces to the host via a high speed 64-bit/133MHz PCI-X bus or through a POS-PHY level 3 compatible streaming bus interface (2x 32-bit, 104MHz).

The 8170 is offered in a 576-PBGA package and is available either leaded or RoHS compliant. Typical power consumption is 4W.

7870 Secure VoIP Processor

The 7870 Secure VoIP Processor supports approximately 1,250 – 5,000 secure full duplex calls. The 7870 is ideally suited to mid-scale SBCs, Media Gateways, Media Servers or packet switches.

The 7870 interfaces to the host via a 66 MHz 32/64 bit PCI bus. It is offered in a 625 PBGA package and is available either leaded or RoHS compliant. Typical power consumption is 2.6W.

Hifn Product Selection Guide

Hifn Products	PCI	Streaming Bus	LZS MPPC	3-DES AES	SHA MD5	RSA DSA	1k-bit RSA SSL signatures per second	IKE main-mode connections per second	Hardware support for public keys up to	Package
HIPP I 7870	■		■	■	■	■	241	159	2K bits	480/625-pin BGA
HIPP II 8170	■	■	■	■	■	■	1000	500	3K bits	576-pin PBGA

7870/8170 Ordering Information

Part Number	Package
7870PP4	480-pin BGA
7870PP6	625-pin BGA
7870PP4-G*	480-pin BGA
7870PP6-G*	625-pin BGA
8170PP5	576-pin BGA
8170PP5-G*	576-pin BGA

*RoHS Compliant

Documentation:
Device Specification
Performance Application Note
DPU Programs Reference Manual
Reference Board Specification
RAM Unit Application Note