

FlowThrough Security for Gigabit Ethernet

APPLIED SERVICES PROCESSOR – 8450



The 8450 Applied Services Processor for Networking ensures data security and integrity with a standards compliant 2-port Gigabit Ethernet solution

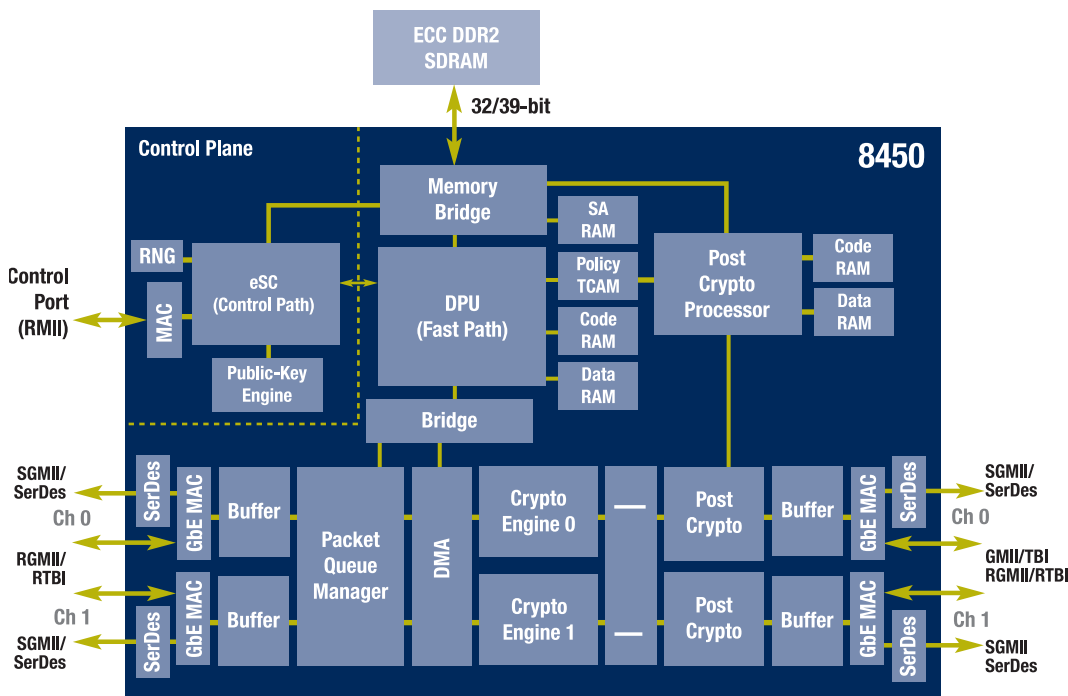
The Hifn 8450 Applied Services Processor (ASP) is the second generation security processor in the FlowThrough™ family. The 8450 builds on the successful and widely adopted 8350 security processor. New to the 8450 are a number of new protocols, features (including IPv6 support) and performance enhancements. The 8450 offers simultaneous IPsec, IPComp, and SRTP security processing. A single packet can be processed through multiple security protocols in a pipelined manner, if required.

The 8450 delivers industry-leading functionality supporting a broad compliment of cryptographic algorithms at multi-gigabit line rates. The FlowThrough security processor includes comprehensive on-chip data plane and control plane software, as well as a robust set of API's for host control of the devices. The 8450 interfaces seamlessly with Gigabit MACs and

PHYs, including most leading network processors, providing a turnkey security solution with minimal development effort.

Hifn's FlowThrough Security Architecture

Hifn's FlowThrough Security Architecture is the cornerstone of a family of solutions that fundamentally changes the way security is built into the network. The FlowThrough architecture enables security processors to sit directly in the data path, eliminating the inefficiencies of existing "look-aside" security designs. The new FlowThrough architecture enables acceleration of the entire data path of the IPsec, IPComp, and SRTP protocols. The advanced architecture incorporates protocol-aware packet processing at the link layer and IP packet layer, and includes full "stack" implementations for multiple security protocols. Hifn's 8450 security processor uses the FlowThrough architecture to ensure very high-performance, low-latency packet processing in Ethernet networking equipment.



PROTOCOLS

- IPsec
- IPComp
- SRTP

ENCRYPTION

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

AUTHENTICATION

- SHA-1
- SHA-256
- MD5
- AES-XCBC-MAC
- AES-CCM
- AES-GCM

COMPRESSION

- IPComp with LZS

INTERFACE BUS

- Host Interface (2x):
 - RGMII/RTBI
 - or GMII/TBI
 - or SerDes
 - or SGMI
- Network Interface (2x):
 - RGMII/RTBI
 - or SerDes
 - or SGMI
- Control Interface:
 - RMII

TUNNELING PROTOCOLS

- IPsec
- ESP/UDP

APPLICATIONS

- VPN Appliances
- Secure NIC Card for Servers
- Security Routers
- Media Gateways

STANDARDS

- RFC 4301 – IPsec
- RFC 3173 – IPComp
- RFC 2395 – LZS with IPComp
- RFC 4303 – ESP Encryption
- RFC 2403 – HMAC-MD5
- RFC 2404 – HMAC-SHA-1
- RFC 3610 – CCM Mode
- RFC 4106 – GCM Mode
- RFC 3711 – SRTP

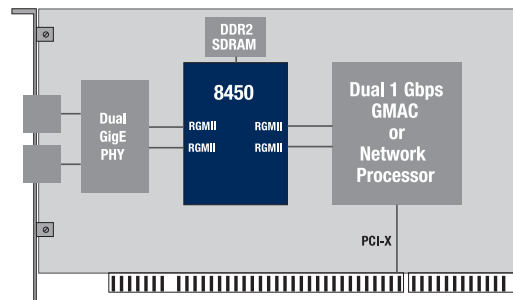
Easy Integration

The Hifn FlowThrough design enables easy integration into a variety of systems, including I/O blades in VPN appliances, Secure Network Interface Cards (NIC's), and Media Gateway appliances.

The 8450 supports four full-duplex 10/100/1000 Ethernet interfaces and is typically inserted between the network processor or GMAC, and an Ethernet PHY. A wide selection of industry-standard Ethernet interfaces, including RGMII/RTBI, SGMII and SerDes, for both the host and network, are supported in the 8450. Additionally, the GMII/TBI interface modes are supported on the host ports. The network- and host-side interfaces may be configured differently, allowing the 8450 to provide interface conversion. These flexible interface options allow glueless interfacing in most systems.

The control interface to the 8450 is typically achieved using in-band Ethernet frames via the Host Interface. An additional 100Mbps Ethernet RMII port allows for an optional out-of-band control port interface to the device if desired. The RMII port may also be used to establish an inter-chip link or control path for multi-chip designs.

The 8450 supports a 32/39-bit DDR2 SDRAM with optional ECC error protection. The memory interface provides for additional SA record storage should more than 200 SAs be required. This feature is also necessary if IKE and/or fragment reassembly is being executed on-chip.



Features and Benefits

Single-chip, low-cost solution

- 4Gbps IPsec/IPComp/SRTP processing (Dual Full Duplex GigEthernet) for large packets
- Minimal part count: one bank of inexpensive DDR2 SDRAM required only for on-chip IKE or extended SAs

FlowThrough security processing

- In-line IPsec, IPComp, and SRTP protocol and algorithm processing
- Streamlined and optimized for VPN applications
- On-chip hardware Public Key accelerator
- Optional on-chip IKE processing
- Complete IPsec/IKE integration for easy system implementation

Optimized for Layer-2 and Layer-3 Security

- 200 SAs supported on-chip
- 1M SAs with external DDR2 SDRAM
- 256 on-chip policy entries (128 per direction)

IETF/IEEE Compliant Functionality

- Supports IPsec ESP, AH & IPComp
- Tunnel and Transport modes
- Performs SRTP packet security processing (AES-CM and SHA-1)
- Full support for IPv4 and IPv6, including IPv4 in IPv6 and IPv6 in IPv4.
- AES (CBC, CTR, CCM, GCM), DES/3DES, SHA-1, SHA-256, MD5, AES-XCBC-MAC

Specifications

- .13µ process, 324 low-profile BGA (19mm square)
- ~2.5W Typical Power Dissipation
- RoHS Compliant package

Ordering Information

Two options are available for these parts. Add the appropriate suffix to the part number. Both options can be added to either part:

- Add “-K” to add an IKE license
- Add “I” to order Industrial Temperature Grade parts

Part Number	Speed	Package
8450HG/3	200 MHz	324 HSBGA (RoHS compliant)
8450HA/3	200 MHz	324 HSBGA (RoHS-5 compliant)