

## Zero Impact Cryptography for Next-Generation ATCA Platforms

### Features

- Complete CPU offload for encryption and compression
- Optional on-chip IKE software stack for additional CPU offload
- Low Power - Less than 10W (typ)
- IPv4 and IPv6 packet processing
- IPsec, SRTP, MACsec
- IPcomp (LZS Compression)
- Hardware acceleration for Suite B, including Elliptic Curve algorithms

### High Performance

- Dual or Quad Port GigE - 2 or 4 Gb/sec FDX
- Up to 2.5 Mpps of packet processing performance
- Support for up to 128K security associations
- Up to 1024 on-board policies
- Large Family of Solutions
- Choice of GigE (AMC.2) or PCI Express (AMC.1) interfaces
- AMC.0 Compliant IPM Controller

### Wide Range of Algorithms Supported

#### Encryption:

- AES-128 and AES-256 in GCM, CBC, CTR modes
- DES/3DES in CBC Mode

#### Authentication:

- SHA (256, 384)
- AES-GMAC (128, 256)
- AES-XCBC-MAC-96
- HMAC-SHA-1
- HMAC-MD5

#### Public Key:

- ECDH-256, 384, 521
- ECDSA-256, 384, 521
- RSA, DH (1024, 2048, 4096)

### Hardware Accelerated Security and Compression Offloads Host CPU, Optimizing CPU Efficiency

The Express DS 4050 family of Advanced Mezzanine Cards leverages the next generation Hifn FlowThrough™ 9155 Applied Services Processor to eliminate all cryptographic and compression overhead for up to 4 full-duplex Gigabit Ethernet ports. The standards-based single width, full height AMC form factor cards support both mid and full size faceplates, and address carrier grade applications requiring wire-speed Ethernet or IP based security, providing off the shelf, production ready solutions for the telecommunications, wireless, VoIP, and IP networking markets. The DS 4050 offers support for Suite B encryption and authentication algorithms, as well as advanced information assurance features, making the DS 4050 ideal for government and military applications.

The DS 4050 advanced FlowThrough architecture enables complete CPU offload for both security and compression, which optimizes host CPU efficiency and application performance. The DS 4050 FlowThrough engines perform security policy processing, security context look-up and cryptography, and compression without impact to the ATCA or MicroTCA host platform processor. The DS 4050 modular architecture enables easy integration and rapid time to market, since packets exit the host network interface as they would in a normal clear text environment before being automatically transformed by the DS 4050. In addition, the establishment of IPsec security associations can be offloaded from the host CPU and performed transparently by running the optional on-chip IKE software stack. Outgoing clear-text packets will automatically start IKE negotiations and establish complete security contexts without host involvement.

### Native Suite B Support and Advanced Containment Delivers Maximum Security

The DS 4050 offers high performance, hardware accelerated Suite B support, making the DS 4050 ideal for government and military applications. The DS 4050 also includes advanced containment features, including signed and verified firmware downloads, key obfuscation, and obfuscation of the external DDR2 memory bus, preventing external memory probing from compromising device security.

### Low Latency Preserves Application Performance

Applications such as packetized voice or video require minimal, deterministic latency to avoid degrading their real time performance. The dedicated FlowThrough engines ensure that performance remains deterministic, rather than dependent on host application processor load, which can vary widely in latency and throughput.

### Low power with High Performance Enables the Green Data Center

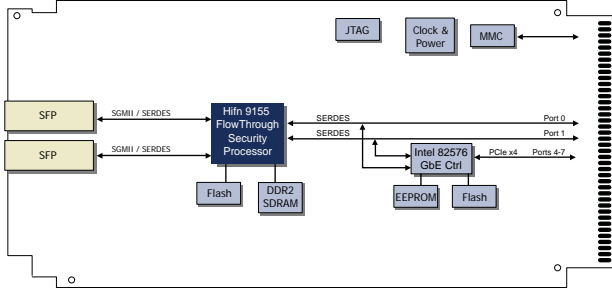
The DS 4050 dedicated encryption and compression hardware reduces the overall system power consumption, yielding huge benefits in cooling and power supply costs.

With a typical AMC power draw of less than 10 watts for all board configurations, the DS 4050 family delivers best in class performance per watt, reducing costs for power and cooling, and helping to enable the green data center.

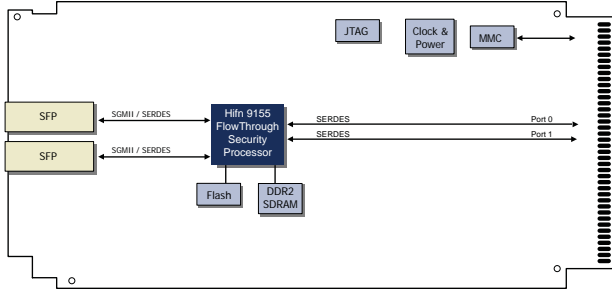


## Block Diagrams

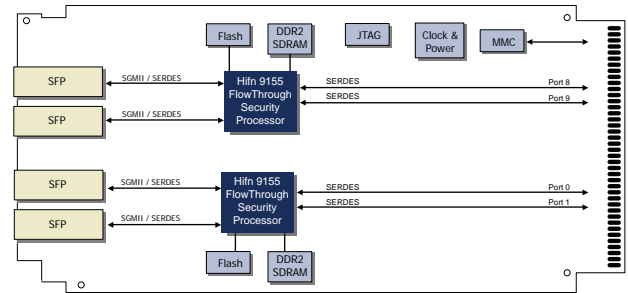
Dual Port PCIe AMC Card



Dual Port SERDES AMC Card



Quad Port SERDES AMC Card



## Applications

### Front Panel

- 2x or 4x Gigabit Ethernet SFP supports SerDes or SGMII
- Link status LED per port – Green
- Activity LED per port - Yellow
- Hot Swap LED - Blue
- Out of Service LED – Red
- In Service/Health LED – Green/Yellow

### Connectivity

- AMC.2 Type E2, Type 2 (GbE 0,1,8,9)
- AMC.2 Type 4 (GbE 8,9,10,11)
- AMC.2 Type E2 (GbE 0,1)
- AMC.1 Type 4 (PCIe)
- AMC.2 Type 2 (GbE 8,9)
- AMC.1 Type 4, AMC.2 Type E2 (PCIe, GbE 0,1)
- AMC.1 Type 4, AMC.2 Type 2 (PCIe GbE 8,9)
- Network ports routed to Rear Transition Module on Ports 17-20

### Form Factor

- PICMG AMC.0 R2.0
- Single Module width
- Mid-Size or Full Size face plates

## Operating Environment

- Power Consumption: Approximately 10W or less typical for all board configurations (preliminary)
- Temperature: 0°C to 55°C
- Relative Humidity:
- 0–95% non-condensing

## Additional Specifications

- Optional PCI Express GMAC using Intel 82576 Dual port PCIe 2.0

## Ordering Information

Part	Description
4050S4	Quad port SERDES with mid-size faceplate
4050S4F	Quad port SERDES with full-size faceplate
4050S2	Dual port SERDES with mid-size faceplate
4050S2F	Dual port SERDES with full-size faceplate
4050SP2	Dual port PCIe with mid-size faceplate
4050SP2F	Dual port PCIe with full-size faceplate

