

### SafeXcel™ IP-160: Intellectual Property (IP)

solution for offloading MACsec security processing through unique data plane processing

Support for cryptographic security is becoming a basic requirement for networks. In a LAN/MAN network, MACsec can provide the required level of security for protecting LAN and Metro Ethernet communications at the link-layer.

### MACsec Protecting the LAN

MACsec is an IEEE 802 standard that specifies how all or part of a LAN network can be transparently secured. MAC Security provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.

## SPECIFICATIONS

#### Applications:

- Allows direct connection to Ethernet MAC; no external host interaction required to determine key material etc.
- Performing MACsec packet transforms including AES-GCM encryption and:
  - SecTAG insertion and removal
  - ICV checking/removal and calculation/insertion
  - Sequence number checking
  - Decoupled control and data plane operation
- Low latency
- The pipe-lined architecture allows the core to accept data back-to-back
- Supports multiple ports, SecY's and Security Channels simultaneously
- Built-in MACsec metering
- Built-in functionality for deciding, and acting on, performing the forwarding,, drop, encrypt or decrypt operation, at full line rates
- Classification capability beyond required for MACsec.
- Capable of servicing a full duplex 10 Gbps Ethernet connection at a clock speed of 250MHz, even for the smallest frame sizes
- Multiple speed grades available with core speed up to 24 Gbps at maximum clock speed
- No external SDRAM or CAM required
- Fully supported by the QuickSec for MACsec toolkit!
- Transaction accurate C-model is available upon request

The MACsec security architecture comprises two main components, an authenticated key agreement protocol defined in 802.1X-REV, and a data plane protocol which protects frames transmitted on the LAN. The data plane protocol is defined in 802.1AE and is known as MACsec. MACsec defines the frame format for data encapsulation, encryption, and integrity protection. MACsec adds a security tag in the frame allowing the receiver of the frame to verify the authenticity, integrity and the timeliness of the frame. MACsec also facilitates optional encryption of the frame.

MACsec capable devices are to become an essential part of LAN and MAN networks. To ensure the security of these networks MACsec functionality will be required on the new generation of network infrastructure switches, from simple consumer switch devices up to high end Carrier grade switches.

As MACsec is the protocol to use for securing Enterprise networks, MACsec functionality will also be needed on end-stations including laptops, PC's printers and network servers. Securing such networks from the inside is becoming more and more important for corporations, and MACsec is ideally placed to fulfill this role.

### High-Performance MACsec Processing

The EIP-160 SafeXcel IP Flow Through MACsec Security Engine's value lies in its unique capability to maximize data plane offloading from a host processor to dedicated hardware. In traditional SoC architectures, hardware assist is usually limited to modules that perform cryptographic security processing under full control of an embedded general purpose processor.

In these architectures, the general-purpose processor still needs to process each frame to some extent — especially at high data rates and for small frame sizes. This approach creates a significant processing burden on the processor, as well as possible overall throughput bottlenecks.

With the SafeXcel IP MACsec Inline Security Engine on the other hand, the general-purpose processor is not involved in processing frames that belong to an existing data flow. This allows the processor to dedicate its clock cycles to data flow setup and other processing tasks. The result is a high-performance MACsec security solution that delivers Gigabit rate processing.

Clock Speed (MHz)	Throughput (Gbps)	Size (kgates)
125	10	379
125	13.3	415
250	20	379/415*
250	26.6	415/475*
375	40	475

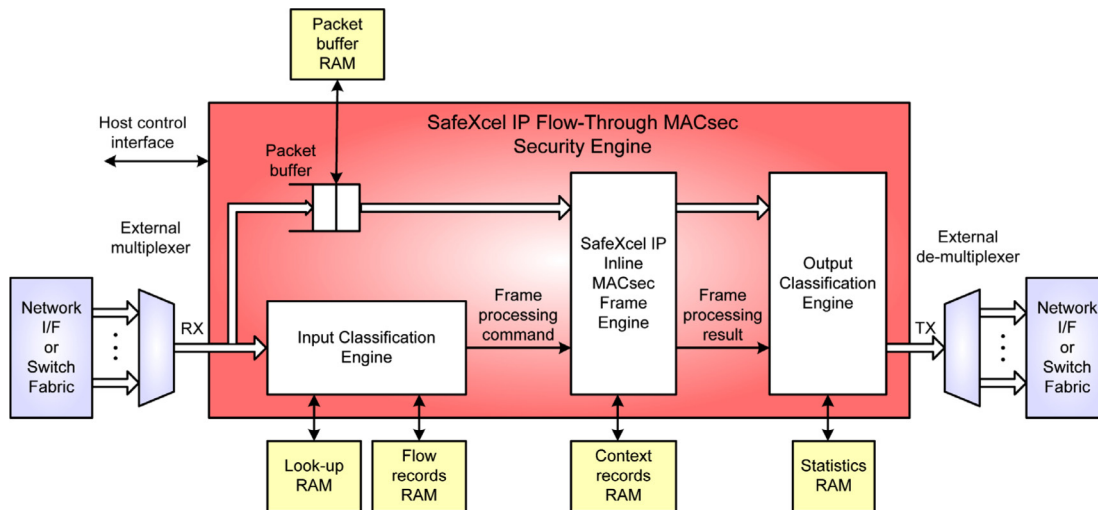
\* Larger value is for slower 130nm technologies.

Note: Throughput numbers are valid for all frame sizes (including Ethernet overhead).

In addition to the above gatecounts, the SafeXcel IP MACsec Inline security engine requires about 50-70 kBytes of on-chip memory, with the exact size, dependent on the total number of secure channels that need to be supported.

### Frame Classification

The EIP-160 SafeXcel IP Flow-through MACsec Security Engine provides complete classification of the incoming frames as required by MACsec and beyond that. This capability is enabled by the engine's unique Frame Classifiers and is not offered by other security IP vendors. Instead of the need to rely on external classification, i.e. classification performed by another processor, the SafeXcel IP MACsec Inline Security Engine includes hardware assist for this timeconsuming task.



For every frame, the Frame Classifiers perform a sanity check, decide how the frame needs to be processed (by the host processor or by the integrated Inline MACsec Frame Engine) or whether it needs to be discarded (filtering). Classifiers also take care of the associated administration, such as transform and flow information updates. The Frame Classifiers autonomously instruct the MACsec Frame Engine which operations need to be performed on the frame. This not only allows the engine to process frames autonomously without requiring per-frame host processor intervention, it also allows the Inline Security Engine to be easily inserted 'in between' the existing connection between the Ethernet MAC and the system's switch fabric.

## MACsec Frame Processing

The MACsec Inline Frame Engine implements various data manipulation functions, including data insertion, data removal, data replacement, data retrieval, and crypto, hash, and checksum operations. The Inline Frame Engine performs such operations on incoming data, as instructed by the Frame Classifier. The MACsec Inline Frame Engine supports the AES-GCM algorithm as defined by the IEEE standard. In order to achieve Gigabit rate throughputs, the MACsec Inline Frame Engine uses a five-stage processing pipeline.

## Integrated Software Support for MACsec Solution

Integrated software support is increasingly becoming a critical success factor for complex SoCs in general and MACsec solutions in particular. SoC vendors and their partners need to be able to provide complete platforms to the OEMs, consisting of integrated hardware and software. In line with this trend, hardware security functionality in a SoC needs to be supported by state-of-the-art software in order to make the SoC successful in its market. The SafeXcel IP MACsec Inline Security Engine has been designed to work seamlessly with SafeNet's MACsec toolkit. The MACsec toolkit's advanced architecture allows data plane processing to be offloaded to an SoC's MACsec Inline Security Engine, thereby maximizing application performance. The toolkit also enforces policies upon the Frame Classifier as part of its control plane functionality. This integration of the MACsec software on your SoC will create an excellent value proposition to your customers.

## TECHNICAL SPECIFICATIONS

### Benefits

- Includes Frame Classification
- Superior throughput across all frame sizes
- Supported by QuickSec for MACsec
- Easy to integrate
- Flexible, modular architecture
- High degree of integration
- World-class support

### Deliverables

- Synthesizable Verilog RTL source code
- RTL test bench
- Simulation script
- Synthesis script
- Driver software
- Extensive Documentation:
  - Product Specification
  - Programmers and Operations Manuals
  - Integration Manual
  - Verification Specification