MAC-SEC-1G

MACsec Protocol Engine for 10/100/1000 Ethernet

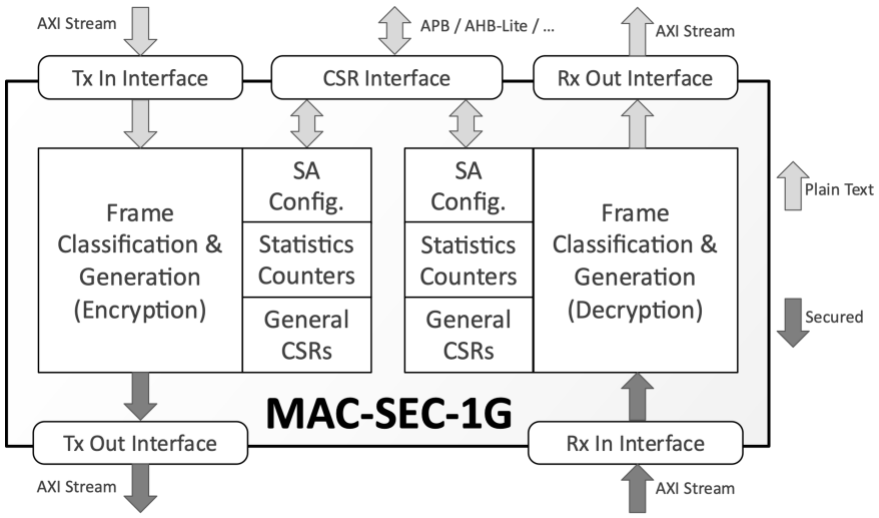
The MAC-SEC-1G IP core implements a compact and configurable custom-hardware protocol engine for the IEEE 802.1AE (MACsec) standard. It supports all cipher suites provisioned by the MACsec standard and the VLAN-in-Clear improvement, and is silicon- and performance-optimized for networks operating up to 1Gbps.

Featuring a configurable number of Security Associations (up to 64k), this protocol engine supports multiple security channels and can implement multiple Security Entities (SecYs). It operates in full duplex mode, at line speed per direction for 1000/100/10 Mbps connections. It does so by implementing a 32-bit wide data path, which provides adequate performance while minimizing silicon resources.

Designed for ease of integration, the MAC-SEC-1G core is a fully synchronous, single-clock domain design that uses standardized interfaces and can be optionally pre-integrated with companion cores available from CAST.

The control and status registers of the core are accessible via a generic 32-bit memory-mapped slave interface. Interface bridges delivered with the core can convert this generic host interface to a generic 8-bit memory-mapped interface or a 32-bit APB, AHB-Lite, Avalon-MM, or Wishbone interface. Packet data are input and output via AXI Stream interfaces with configurable data width, enabling direct connection to Ethernet MACs, PTP timestamping units, or other higher-layer protocol engines. Interface bridges and a DMA engine capable of driving the AXI Stream interfaces are available separately. They can be used in cases where moving data to and from the core is preferable over a memory-mapped bus. The core can be delivered pre-integrated with the Low-Latency Ethernet MAC or any Ethernet TSN cores available from CAST.

Block Diagram



FEATURES

MACsec Protocol Engine

- Compliant with IEEE 802.1AE-2018 and IEEE 802.1AEbw
- Implements both GCM-AES and GCM-AES-XPN modes with 128- and 256-bit keys.
- Multiple Security Channels, Security Associations, and Security Entities
  - The maximum number of security associations is synthesis-time configurable in the range of 1 to 64k.
- Supports 802.1Q Tag in the Clear (VLAN-in-Clear) as defined by CISCO's WAN MACsec

Performance and Size

- Compact 32-bit data path
- Full-duplex, line-speed operation at 10/100/1000 Mbps

Easy to Integrate

- AXI stream interfaces with configurable data width allow direct connection with eMAC or higher-layer protocol engines
- Uses a generic 32-bit slave interface & bridges to 32-bit APB, AHB-Lite, Avalon-MM, or Wishbone, or to an 8-bit generic microcontroller interface.
- Reports status, statistics, & errors in CSRs
- Companion cores from CAST:
  - DMA for integration as a memory-mapped peripheral.
  - Low-Latency Ethernet MAC
  - UDP/IP and TCP/IP hardware stacks
  - TSN Endpoints and Switches

Straightforward to Implement

- Available in LINT-clean, scan-ready, synthesizable RTL source code format or as a targeted FPGA netlist
- Single clock-domain design with no multi-cycle or false paths
- Platform-Independent – Can be implemented on any FPGA device or ASIC technology

Applications

The MAC-SEC-1G core provides hardware-accelerated MACsec protection for end-to-end transmission in industrial, automotive, IoT edge, and other devices with Ethernet connectivity. While it works well with third-party cores, the MAC- SEC-1G is especially well suited for use with the Low-Latency eMAC, the UDP/IP and TCP/IP hardware stacks, and the TSN Endpoint and Switch cores available from CAST. These can be licensed as a pre-integrated subsystem, enabling the rapid, low-risk development of secure Ethernet connections.

Implementation Results

The MAC-SEC-1G is a purely digital IP core and can be mapped in any ASIC or FPGA technology. The silicon resources required for its implementations depend on the core configuration. Please contact CAST to get accurate characterization data for your target application and core configuration.

Deliverables

Consistent with CAST's quality standards, this core has been rigorously verified, is LINT-clean and scan-ready, and is delivered with everything required for a trouble-free implementation. It is available in System Verilog RTL source code or as a targeted FPGA netlist, and its deliverables include a sophisticated testbench, sample synthesis and simulation scripts, and comprehensive documentation.

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.