

General Description

Implementation of the LAN security standard IEEE 802.1ae (MACsec) requires the NIST standard AES cipher in the GCM mode for encryption and message authentication, as well as header parsing and formatting operations on the transmitted and received packets. MACsec Security Processor (MSP) IP cores by IP Cores, Inc. are designed for high data rates and implement complete line-rate packet processing with no per-packet CPU intervention. The MSP7-64/256 cores are tuned for 10-25 Gbps applications in the FPGA and ASIC technologies that require 256 bit AES keys.

The design is fully synchronous and available as RTL source code.

Key Features

Small size combined with high performance:

- 10 Gbps performance at the 156+ MHz clock rate
- 25 Gbps performance at the 390+ MHz clock rate

Flow-through design with back-to-back packet processing

- 64 bytes shortest packet at full data rate
- 16,000 bytes maximum packet size

Low latency: TBD¹ clocks input-to-output on encryption, TBD clocks for decryption.

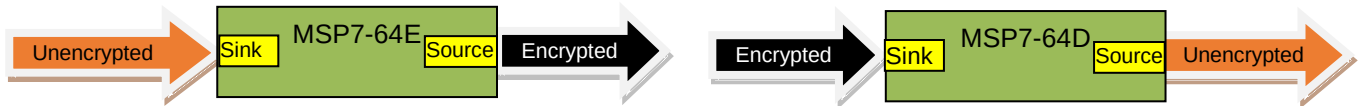
Delivered as a set of two cores: MSP7-64E implements encryption for egress (Tx); MSP7-64D implements decryption for ingress (Rx). MSP7-E and MSP7-D within this document are simply shorter notations for the same cores.

- Each core utilizes two clocks: one for the datapath and one for control

¹ The latency is fixed (does not vary from packet to packet), is in the range of 20..100 clocks, and depends primarily on the ASIC technology node selection or FPGA family

64-bit aligned² wide AXI-S data interface with flow control.

- The MSP7-64E presents a sink interface to the unencrypted side, source interface on the encrypted side.
- MSP7-64D presents a sink to the encrypted, source to the unencrypted.



The core is designed for multiple Secure Channel (SC)³, 2-4 Secure Associations (SAs) per SC.

Support for the 256 bit AES key per IEEE 802.1AEbn standard

Support for Extended Packet Numbering per IEEE 802.1AEbw (GCM-AES-XPB-128, GCM-AES-XPB-256).

Support for IEEE 802.1AEcg Draft Amendment 3 (Ethernet Data Encryption devices)

Support for the VLAN tags in the clear: move or copy the C-Tag and S-Tag in the header.

Bypass for the PTP data.

AHB-Lite interface for control.

Provides MACsec header parsing and modification:

- Insertion and removal of the SecTag including the packet number (PN) and an optional SCI
- RX packet validation
- Insertion, validation and removal of the ICV
- Replay protection based on the PN windowing

Includes key storage and expansion.

Support for Galois Counter Mode Encryption and authentication (GCM-AES-128, GCM-AES-256), Galois Message Authentication (GMAC)

Optional external statistics block with glueless interface to the core.

² A new data frame shall always start at the MSB of the data bus

³ Multiple classification options available covering the range from few SCs to few thousand SCs. This configuration uses external pins for classification on egress, SCI for classification on ingress.

Test bench provided.

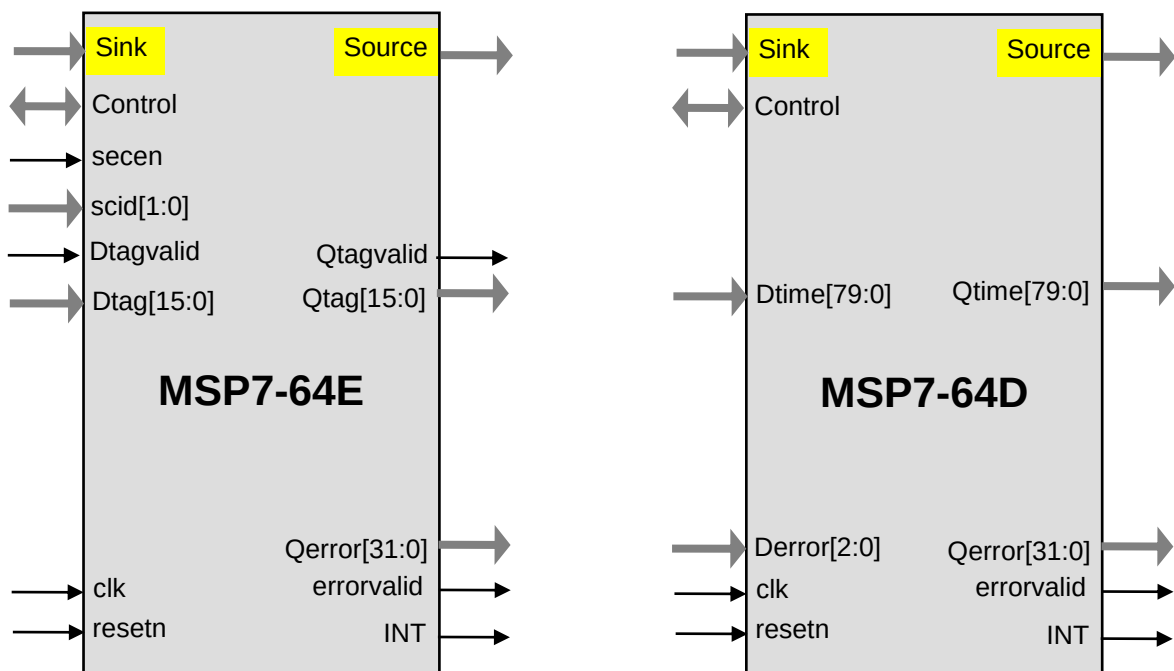
Sample SDK for core control and 802.1X implementation.

Deliverables include test benches and optional NIST algorithm validation.

Applications

- IEEE 802.1ae MACsec

Symbol



Pin Description

Name	Type	Description
<i>Generic</i>		
clk	Input	Core clock signal. Used for both Sink and Source.
reset	Input	Core reset signal, active HIGH.
<i>Sink Interface is an AXI-S interface with continuous aligned stream.</i>		
<i>MACsec out of band signaling</i>		
Derror[2:0]	Input	Error signal. MSP7-64D only. Allows the core to receive the Rx error indicators (typically FCS and reception errors) from the MAC. The core does not interpret these and simply passes them through to the source interface alongside with its own errors. Sampled when I_tlast is asserted.
Qerror[31:0]	Output	Error signal. Asserted once for every packet, might indicate the need for the external circuitry to take specific action. Also used for the glueless interface with the statistics block.
errorvalid	Output	Qerror value is valid. If the packet is not suppressed, asserted simultaneously with I_tlast .
scid[1:0]	Input	Secure channel selection for the packet. Valid if scen is asserted.
Dtagvalid	Input	PTP tag (Dtag) valid. MSP7-64E only. PTP tag is bypassed through the core. Asserted simultaneously with the first word of the packet.
Dtag[15:0]	Input	PTP tag. MSP7-64E only. Valid when Dtagvalid is asserted.
Qtagvalid	Output	PTP tag (Qtag) valid. MSP7-64E only. Asserted simultaneously with the first word of the packet.
Qtag[15:0]	Output	Bypassed PTP tag. MSP7-64E only. Valid when Qtagvalid is asserted.
Dtime[79:0]	Input	PTP time stamp. MSP7-64D only. To be asserted simultaneously with the first word of the packet. The time is bypassed by the core.
Qtag[79:0]	Output	Bypassed PTP time stamp. MSP7-64D only. Valid simultaneously with the first word of the packet.
secen	Input	"Controlled port" (enable encryption for this packet).
<i>CPU interface is APB, AHB-Lite, or AXI-lie</i>		

Description

The MSP7 implementation fully supports the IEEE 802.1ae (MACsec) algorithm for 256-bit bit keys (IEEE 802.1AEbn), including AES support in Galois Counter Mode (GCM) per NIST publication SP800-38D

<http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf> and extended packet number per IEEE 802.1AEbw.

Tx Processing (MSP7-64E)

On encryption, for each frame the core:

- Selects a proper SC based on external input
- Looks up the current SA key
- Inserts the SecTag, including the PN and an optional SCI
- Encrypts and authenticates the frame, based on the values on the E and C inputs
- Appends the ICV tag to the packets
- Updates the PN

Rx Processing (MSP7-64D)

On decryption, for each MACsec frame the core:

- Obtains the SC index from the SCI (or fixed if SCI is not present) and looks up the current SA key
- Validates the SecTag and SCI, if present
- Removes the Ethernet padding from frames shorter than 64 bytes if indicated by the SL field
- Checks that the packet number PN is within the PN window
- Decrypts the frame, if encrypted
- Calculates the ICV tag, if the frame is authenticated, and compares to the one in the frame
- Removes the ICV tag, appended to the frame
- Updates the PN window

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Expected results
- User Documentation
- Vectors for testbenches
- Optional GCMVS NIST validation
- Optional UNH validation



www.ipcores.com

MSP7-64 MACsec Core

10G-25G, 64 bit interface for FPGA or ASIC

Contact Information

IP Cores, Inc.

3731 Middlefield Rd.

Palo Alto, CA 94303, USA

Phone: +1 (650) 815-7996

E-mail: info@ipcores.com

www.ipcores.com