IEEE 802.1ae MACSec IP Core for 40Gbit Ethernet

Preliminary Product Description

September 2015

algotronix
130-10 Calton Road
Edinburgh EH8 8JQ
Phone: +44 131 556 9242
E-mail: cores@algotronix.com
URL: www.algotronix.com

Algorithm	**IEEE 802.1AE MACSec**
Test Method	Algotronix provided testbench
Performance/Area	Tradeoff via compilation options.
Deliverables	VHDL with testbench. Optimizations for Xilinx FPGAs.

Multiple SecY MACSec Core for Secure Ethernet Communications

Features

- Complies with IEEE 802.1AEbn-2011 standard
- Can provide multiple SecYs to Support Multi-Access LANs (IEEE802.1AE, section 11.8)
- Performance of 40Gbit/sec with 324MHz clock
- Based on the Algotronix AES-GCM-40G encryption core
- Supports 256 bit keys
- Targets all modern FPGA families from Xilinx.
- Supplied as easily customizable portable VHDL to allow customers to conduct their own code review.
- Supplied with comprehensive test bench containing a behavioral model of MACSec developed by Algotronix.

Potential Applications

- Government/Military secure communications
- Secure Ethernet networking Metro Area Networks
- Bridges and routers
- Carrier Ethernet systems
- Enterprise systems
- Test equipment

General Description

Ethernet is a ubiquitous, efficient and cost-effective transport mechanism for unified communication of voice, data and video over a shared medium, but it was not designed with secure networks in mind and is not inherently secure. Media Access Control Security (MACSec) has been specified by the IEEE as a layer 2 security scheme for Ethernet. It is compatible with the revised IEEE 802.1X-2010 specification for port based Network Access Control and provides additional security for all Ethernet traffic types. MACSec can be applied to any Ethernet network and as well as its use in datacenters and office networks is eminently well suited to secure to military and governmental communications systems. MACSec provides an exciting opportunity to add standards based security to Ethernet connected embedded systems.

In the MACSec scheme nodes on a network form a set of trusted entities. Each node can receive both encrypted and unencrypted messages, and the system policy can dictate how each is handled. The MACSec Security Entity (SecY) has a single secure channel for transmit and multiple secure channels for receive. This means that a single SecY is unable to partition the nodes it transmits data to into separate groups and use different keys for each group. Therefore, for example, if it transmits messages to station A and station B, station B has the key necessary to decrypt messages for station A as well as its own messages. The Multi-Access LAN section of the standard (section 11.8 and specifically 'Station A' in diagram 11-15) supported by this core extends basic MACSec to include multiple SecYs and removes this restriction. The core provides multiple 'virtual' SecYs using a single hardware encryption engine.

In the case where, for example, four 10G Ethernet channels are multiplexed onto a single 40G channel and protected by MACSEC the multiple SecY feature could be used so that each 10G channel was assigned to a different SecY and the MACSEC processing would be logically the same as if the four channels had not been multiplexed together. Specifying a larger number of SecYs will result in increased usage of FPGA block RAM to store the state information for each SecY but does not significantly increase data path resources. If the multiple SecY feature is not required then only one SecY need be used.

The MACSec core is a high performance pipelined implementation of IEEE standard 802.1AEbn, the 'bn' amendment provides for the use of 256 bit AES keys. The core is built on Algotronix' pipelined implementation of the AES-GCM encryption algorithm which itself builds on our G3 AES core. This release of the MACSec core supports operation at 1Gbit/sec and 10Gbit/sec. The core is designed to scale up to a throughput of 40GBit/sec on FPGAs by changing the external bus width, proportion of clocks used to transfer data and degree of pipelining as shown in Table 1. At the heart of the MACSEC core AES-GCM encryptors are operating with a 128 bit internal data path and 1 compute unit for 1Gbit performance, a partially unrolled pipeline of 5 (for 128 bit keys) or 7 (for 256 bit keys) compute units for 10Gbit performance and a fully unrolled pipeline of 10 or 14 compute units for 40GBit performance.

Performance	External Bus Width	Active Clocks	Clock Frequency
1GBit/sec	64	2/10 (128 bit key) or 2/14 (256 bit key)	100MHz
10Gbit/sec	64	All	156.25MHz
40Gbit/sec	128	All	324Hz

Table 1: Performance Options.

The Algotronix MACSec core is supplied with a VHDL testbench which generates a sequence of test packets and compares the responses of the IP core to the output generated by a behavioral model of MACSec. It is supplied as VHDL source code and can be configured using a number of VHDL generic parameters to select only those features which are required in order to conserve area. The MACSec core provides both transmit and receive channels. The core is an easy to use fully synchronous design with a single clock and separate flow control on the transmit and receive channels. The core has been designed for efficiency in modern FPGAs and makes full use of FPGA specific features such as dual port memory blocks.

Performance and Area

The core provides many options to allow the user to trade off area against throughput and latency and the FPGA architecture and speed grade also has a strong bearing on the results achieved. In addition, both the core itself and the FPGA manufacturer's design tools are regularly updated resulting in area and maximum clock frequency results rapidly becoming out of date. Contact us with the desired throughput, target FPGA family and speed grade, and we will work out the best core configuration and use the latest FPGA design tools and core source code to provide estimates of the attainable clock frequency and area in the required configuration.

Example statistics for the 1, 10 and 40G configuration of the core are provided below.

Family	Example Device	Fmax (MHz)	FF	LUT	Memory LUT	GCLK	BRAM (18K)	Throughput (GBit/sec)	Design Tools
Zynq	XC7Z100ffg1156-1	125	14618	13196	784	1	32.5	1Gbit//sec	Vivado 2014.4

Table 2a: Example implementation statistics for Multiple SecY MACSec 1Gbit/sec, 256 bit Key, 32 Secure Channels implemented, 8 transmit routing table entries implemented, 16 SecYs, 125MHz Clock, ‘Push Button’ flow with Fmax specified by clock constraint. AES SBoxes implemented in LUTs.

Family	Example Device	Fmax (MHz)	FF	LUT	Memory LUT	GCLK	BRAM (18K)	Throughput (GBit/sec)	Design Tools
Kintex Ul-trascale	XCKU035fbva900-1-i	156.25	18348	24465	456	1	165 (82.5 36K BRAM)	10Gbit//sec	Vivado 2015.1

Table 2b: Example implementation statistics for Multiple SecY MACSec 10Gbit/sec, 256 bit Key, 32 Secure Channels implemented, 8 transmit routing table entries implemented, 16 SecYs, 156.25MHz Clock, ‘Push Button’ flow with Fmax specified by clock constraint. AES SBoxes implemented in RAMs.

Family	Example Device	Fmax (MHz)	FF	LUT	Memory LUT	GCLK	BRAM (18K)	Throughput (GBit/sec)	Design Tools
Kintex Ul-trascale	XCKU035fbva900-1-i	156.25	16220	21776	456	1	133 (66.5 36K BRAM)	10Gbit//sec	Vivado 2015.1

Table 2c: Example implementation statistics for Multiple SecY MACSec 10Gbit/sec, 128 bit Key, 32 Secure Channels implemented, 8 transmit routing table entries implemented, 16 SecYs, 156.25MHz Clock, ‘Push Button’ flow with Fmax specified by clock constraint. AES SBoxes implemented in RAMs.

Family	Example Device	Fmax (MHz)	FF	LUT	Memory LUT	GCLK	BRAM (18K)	DSP48	Throughput (GBit/sec)	Design Tools
Virtex 7	XC7VX485tffg1761-3	324	21205	37492	1310	1	48 (24 36K BRAM)	2	40Gbit//sec	Vivado 2015.1

Table 2d: Example implementation statistics for Multiple SecY MACSec 40Gbit/sec, 256 bit Key, 32 Secure Channels implemented, 8 transmit routing table entries implemented, 16 SecYs, 324MHz Clock, 'Push Button' flow with Fmax specified by clock constraint and specific implementation settings. AES SBoxes implemented in LUTs.

Functional Description

There are two main functional blocks in the MACSec design. The Receive path takes MACSec encapsulated packets, captures the header to determine the Secure Channel Identifier (SCI) and other information and decrypts and authenticates the packet using AES-GCM. It then removes the MACSec encapsulation and provides a secure copy of the original non-MACSec packet to the system through the controlled port. The receive operation reduces the size of incoming packets, therefore the bandwidth requirement on the output side is lower than that on the input side. Receive can also transfer non-MACSec protected packets straight through without processing and deliver them to the uncontrolled port. There are a number of interacting options in the control memory which specify the details of how packets will be processed: the details are in the flowchart in Figure 10-5 of the IEEE802.1AE standard.

The transmit data path adds MACSec encapsulation to an incoming packet, encrypts it using AES-GCM, which adds an Integrity Check Value (ICV), and outputs the data (Figure 2). The transmit operation increases the size of incoming packets, therefore the output side bandwidth requirement is higher than that on the input side. The throughput number specified for the MACSec core refers to the MAC side of the system which deals with encapsulated packets. For example, a 10Gbit/sec MACSec unit will not be able to cope with a sustained 10Gbit/sec stream of minimum sized un-encapsulated packets on the system input since this would require more than 10Gbit/sec at the Ethernet MAC. The details of transmit channel processing are shown in the flowchart in Figure 10-4 of the MACSec standard.

There is no fixed relationship between the time of packet arrivals on the transmit and receive channels and each channel can itself contain more than one packet at different stages in the processing pipeline. With multiple packets in the processing pipeline and multiple SecYs it is possible that different SecY information will be needed at different stages in the pipeline. Thus, updating the SecY control information from the processor needs to be done with care to avoid spurious, partially updated, information being used. The device driver software should disable the controlled port prior to updating SecY information and this can be done with a single write to the control memory making it an atomic operation.

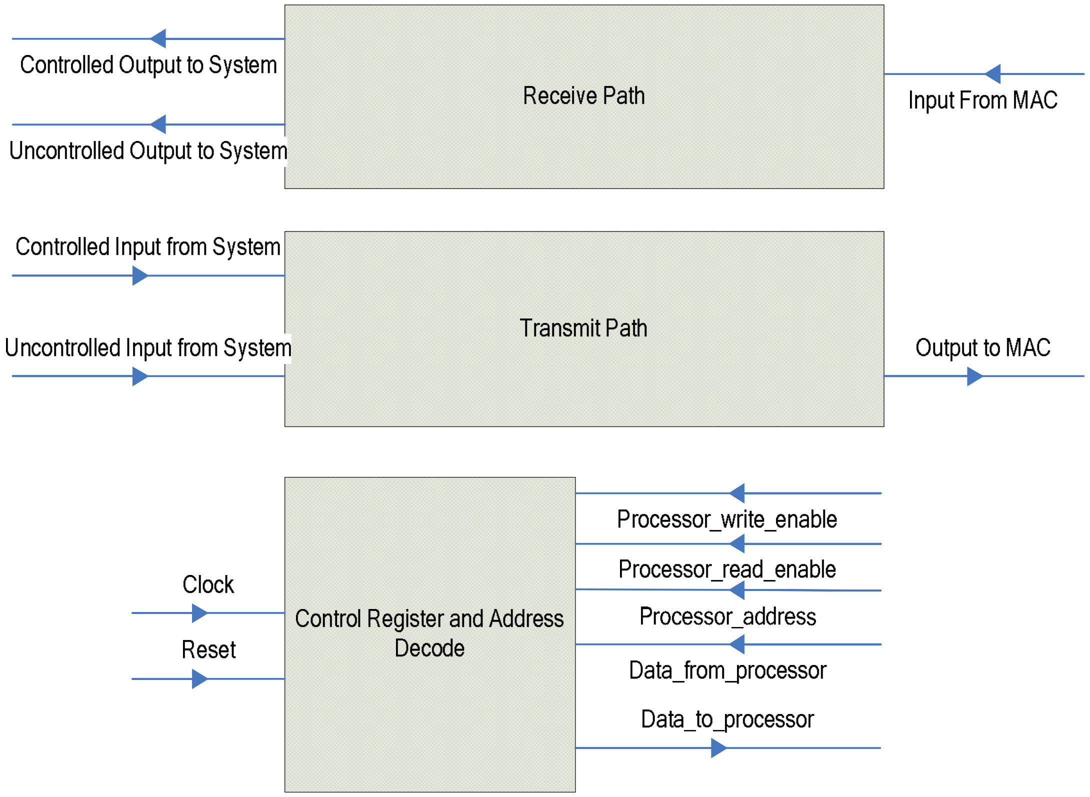

Figure 1, MACSec Block Diagram

MACSec operates on Ethernet packets on the system side of the Ethernet MAC. It provides separate transmit and receive channels between the MAC and the host system which operate independently. On the system side MACSec provides two ports for each channel. The controlled port is for packets which are subject to MACSec security and the uncontrolled port is for packets which are to pass straight through MACSec.

The MACSec unit must also be provided with the keys for use by the AES-GCM encryption units within the transmit and receive channel. On the receive channel the incoming packets may come from many different sources and be associated with many different secure channels - each of which has its own key. Key agreement between the SecY and remote SecYs with which it wishes to communicate is outside the scope of the 802.1AE MACSec standard: key agreement could be handled by software implementing IEEE802.1X port based authentication or in an ad-hoc scheme using a protocol like Internet Key Exchange (IKE). The MACSec IP core relies on the host system to provide it with the correct keys for each secure channel.

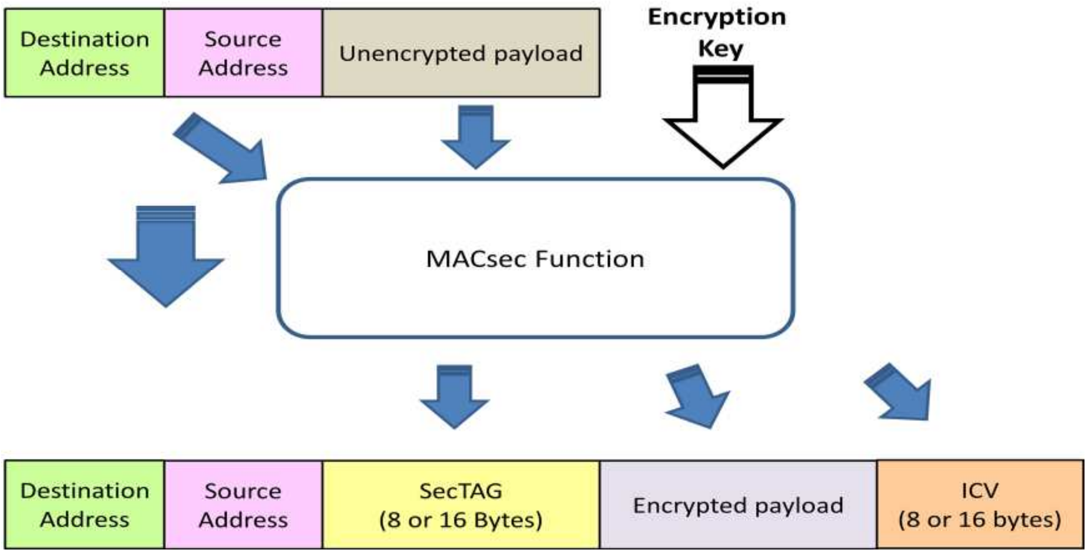

Figure 2, MACSec Frame Format

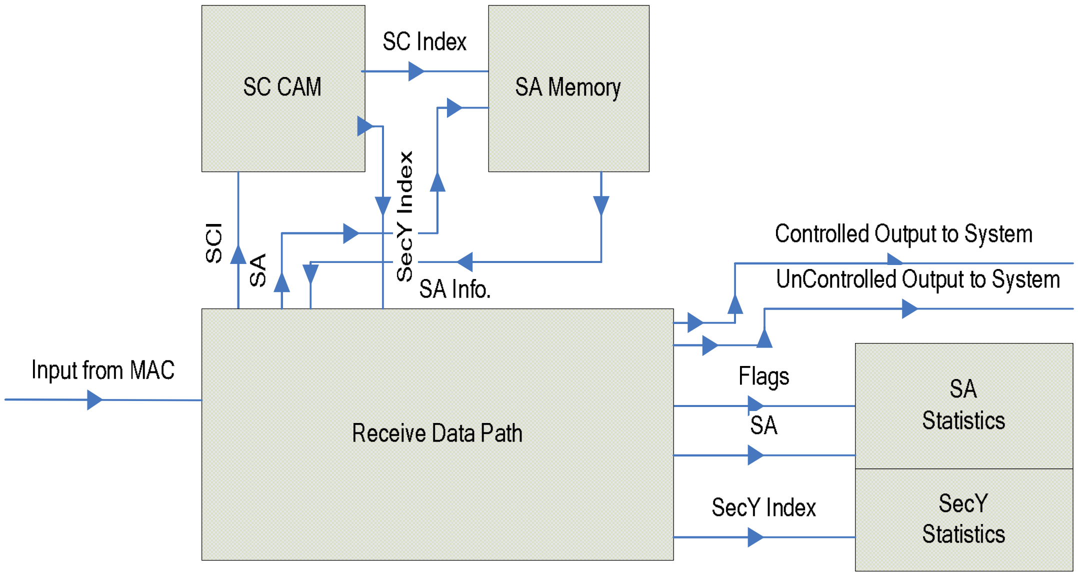

Figure 3. Receive Channel Block Diagram

Receive Channel

The Secure Channel CAM (SC CAM) is used to look up the Secure Channel Identifier (SCI) extracted from the SecTag in the packet header (or a default SCI in the case of a point to point link where the SecY only communicates with one other SecY) and determine the corresponding SecY and Secure Channel (SC). A total of 64 Secure Channels, each with 4 Security Associations (SAs) can be supported by the present core. The core can be customized to provide a different number of secure channels on request. When combined with the SA information from the packet SecTag the SecY and SC determined from the CAM provide sufficient information to find the cryptographic key to be used to decrypt the packet within the SA Memory.

The receive data path ensures that the packet has not been corrupted by checking the Integrity Check Value (ICV) computed by AES-GCM decryption against the expected value supplied with the packet. It also checks the packet number to guard against replay attacks. The original Ethernet frame can then be rebuilt from the decrypted plaintext and passed to the secure controlled port, while the Statistics block updates various counters (implemented as memory locations within FPGA RAM blocks) to track how many packets have been accepted or rejected and the reasons for rejection.

The MACSec core also provides an additional filtering function on the receive channel uncontrolled port. In Figure 10-5 of the IEEE 802.1ae MACSec standard the secure frame verification process is shown as a packet coming from a common port, being copied unchanged to an uncontrolled port and in parallel being processed through the MACSec logic to a controlled port. The problem with this logical model is that copying data unchanged to the uncontrolled port will double the worst-case throughput that the system needs to cope with. This is obviously undesirable for high throughput systems. Therefore, before forwarding packets to the uncontrolled port the MACSec IP core examines the packet header - if the Ethertype is MACSec or if validate_frames is not set to 'strict' the packet will not be forwarded to the uncontrolled port. This modification means that each input packet will appear either on the controlled or the uncontrolled port, but not both, so that the output throughput matches the input throughput and only a single output bus is required with one bit signals specifying whether the packet on the output bus is for the controlled or uncontrolled port.

In the model of the MACSec standard this filtering to eliminate duplicate packets on the Uncontrolled port is regarded as part of the surrounding system but in a hardware implementation it is more efficient to include it within the MACSec IP core. To implement the standard exactly with no filtering of packets to the uncontrolled port simply use wiring outside the core to copy the common input port to a new uncontrolled port and ignore the uncontrolled port output from the IP core.

Transmit Channel

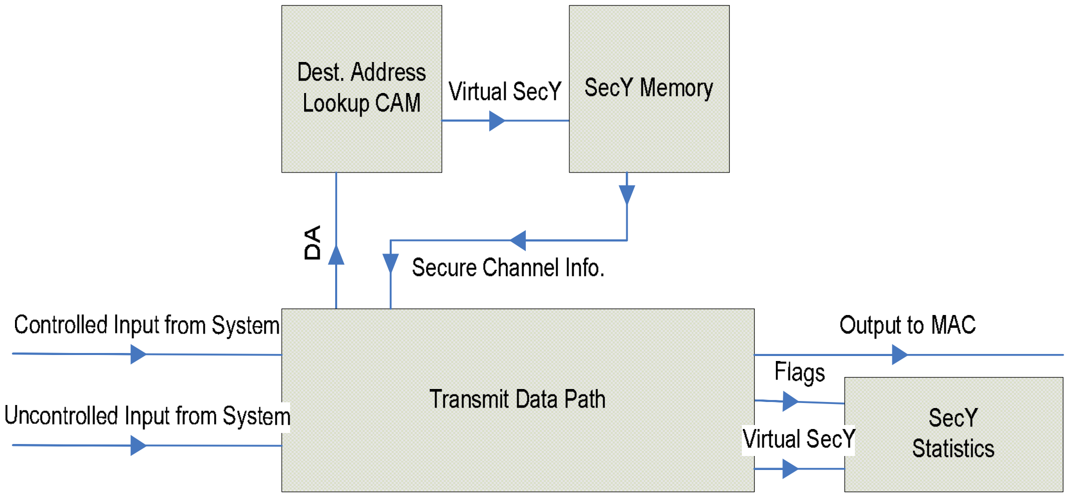

Figure 4. Transmit Channel Block Diagram

To support multiple SecY configurations the transmit channel design includes a CAM which determines the appropriate virtual SecY to use for a given packet based on its Destination Address. Multiple destination addresses can be associated with the same SecY. In the logical view in Figure 11-15 of the standard this CAM would be outside of the SecYs of Station A. It functions as a demultiplexer which routes packets to the ports associated with either the left hand or the right hand SecY within Station A. Customers have found the CAM to be convenient but a closer mapping to the standard might be obtained by doing this demultiplexing outside the MACSec IP core and providing extra signals on the input port so external circuitry could specify which of the Virtual SecYs to use for transmit. **Algotronix would be happy to customise the core to remove the CAM and have the SecY specified by an external signal if this approach is preferred.**

The receive channel supports 64 Secure Channels each corresponding to a potential remote SecY. Therefore it seems logical to provide 64 entries in the Destination Address lookup CAM. If there is a match between the destination address field of the packet being transmitted and an entry in the CAM the index of the corresponding Virtual SecY will be returned. The core will support up to 8 Virtual SecYs. The CAM will return SecY 0 for any packets whose destination address does not match an entry in the CAM to provide a default SecY for any destination address not explicitly assigned to a SecY. Without the default SecY a packet whose destination address did not match would be regarded as an error condition and new ad-hoc error handling outside of the MACSec standard would be needed.

Some of the virtual SecYs may have ControlledPortEnabled set to false. If a packet enters on a disabled SecY it will be dropped. With one SecY packets could be prevented from entering when ControlledPortEnable was false but this is not practical when there is a single input port shared by multiple SecYs and it is not known which SecY a packet will use until the header has entered MACSec.

Compilation Options

The core can be configured easily using a set of VHDL generic parameters. Normally, it is unnecessary for users to modify the design source code although the code is supplied and they are free to do so if they wish. Algotronix can also customise the core as a service for users with particular requirements which are not met by the standard product. Configuration settings like the number of Secure Channels and SecYs supported can be changed through constants in the source code file macsec_package.vhd but this requires re-verification of the core in the new configuration and may alter the memory map so is better handled by Algotronix than by the user.

- **macsec_configuration -** Specifies the configuration of the MACSec core. Currently the only option for the 40G core is MACSEC_40G_256, the MACSEC_40G_128 option will be provided in a future release.
- **target_device** – Specifies the Xilinx FPGA family to be targeted. For the 40G option a modern high performance FPGA family such as Virtex 7 or Virtex Ultrascale will be required.

Core I/O Signals

The core I/O signals have not been fixed to specific FPGA device pins to provide flexibility for interfacing with user logic. Descriptions of all ports are provided in Table 3.

Signal	Signal Direc-tion	Description
Timing Signals		
clock	input	Clock – active on rising edge
reset	input	Reset – active high. For Xilinx FPGA implementation, unless security considerations mandate an asynchronous reset, it is recommended to specify that the reset signal is implemented synchronously a synchronous reset can result in reduced area and improved performance.. A configuration constant USE_ASYNCHRONOUS_RESET to specify the style of reset is provided in aes_package.vhd.
receive_channel_enable	input	Clock enable for flow control on the path from MAC to system. This signal can be used to pause the core when the user design is not ready to supply or to accept data.
transmit_channel_enable	input	Clock enable for flow control on the path from system to MAC. This signal can be used for flow control to pause the core when the user design is not ready to supply or to accept data.
receive_port_output_cycle	output	High when controlled or uncontrolled data is being transferred to the receive channel output port.
transmit_controlled_port_input_cycle	output	The core can block data transfer into the transmit controlled port by bringing this signal low. Future releases may use this signal to enforce an inter packet gap to provide for packet expansion in the transmit channel as the MACSEC overhead is added.
transmit_uncontrolled_port_input_cycle	output	The same function as transmit_controlled_port_input_cycle but for uncontrolled port packets.
Processor Interface		
write_enable	input	Write strobe for processor to write the data on data_from_processor to control memory.
read_enable	input	Read strobe for processor to read data from status memory. There is a one clock cycle delay before the data becomes available on data_to_processor.
address	input	Address of control/status memory location to be accessed
data_from_processor	input	Data bus connection (32 bit bus)
data_to_processor	output	Data bus connection
Data I/O Connections		
first_input_from_mac	input	High when the first word of a packet is being transferred
final_input_from_mac	input	High when the last word of a packet is being transferred
final_input_from_mac_width	input	Indicates the number of bytes in the last word of a packet which are used to transfer data. Packets do not need to be an integral number of 32 bit words long so the final word is often incomplete.

input_from_mac(127:0)	input	Input data.
first_output_to_mac	output	High when the first word of a packet is being transferred
final_output_to_mac	output	High when the last word of a packet is being passed
final_output_to_mac_width	output	Indicates the number of bytes in the last word of a packet which are used to transfer data. Packets do not need to be an integral number of input words so the final word is often incomplete.
drop_output_to_mac	output	High when final_output_to_mac is true if the received packet should be dropped. This can happen if the input packet becomes oversized after adding the additional MACSec information.
output_to_mac(127:0)	output	Output data.
first_controlled_port_input_from_system	input	High when the first word of a packet to be protected by MACSec is being transferred
first_uncontrolled_port_input_from_system	input	High when the first word of a packet to be passed through unchanged is being transferred
final_input_from_system	input	High when the last word of a packet is being passed
final_input_from_system_width	input	Indicates the number of bytes in the last word of a packet which are used to transfer data. Packets do not need to be an integral number of 32 bit words long so the final word is often incomplete.
input_from_system(127:0)	input	Input data.
first_controlled_port_output_to_system	input	High when the first word of a MACSec protected packet is being transferred. At this point the MACSec encapsulation has been removed and the packet is not encrypted.
first_uncontrolled_port_output_to_system	output	High when the first word of an unprotected packet is being transferred
drop_output_to_system	output	High when final_input_to_system is true if the received packet should be dropped. This signal is only valid on the final word of the packet because MACSec cannot tell whether a packet should be dropped until it has processed the ICV at the end of the packet.
final_output_to_system	output	High when the last, potentially partial, word of a packet is being transferred
final_output_to_system_width	output	Indicates the number of bytes in the last word of a packet which are used to transfer data. Packets do not need to be an integral number of 32 bit words long so the final word is often incomplete.
output_to_system(127:0)	output	Output data.

Table 3: Core I/O Signals.

Memory Map for MACSEC 40G

The addresses in this description select 32 bit data words. If the processor running the device driver software addresses bytes bit 0 of the MACSec core address bus would be connected to bit 2 of the processor address bus (and so on).

The most significant bit of the address bus selects between the memory mapped resources for the transmit and receive channel. The transmit channel requires fewer resources than the receive channel so the global resources shared by both channels are also mapped into the transmit channel address space.

Address Space	Address(15)
Receive Channel Resources	0
Transmit Channel and Global Resources	1

Table 4: MACSec Top Level Address Spaces.

Address bits (14:13) are used to select a major resource within a channel, the address segments corresponding to each resource have higher values the further 'right' the resource is in the logical enter on the left, leave on the right flow of a packet through the channel.

Receive Address Space	Address(14:13)
Secure Channel CAM and data	00
Decryption Unit Key Memory	01
SecY Statistics Memory	10
Security Association Memory	11

Table 5: MACSec Receive Channel Address Space.

The address layout for the Transmit Channel follows that for the Receive Channel. There are no SA Statistics in the Transmit channel (because there is only one SA per SecY) so that section of the address space has been used to fit in the global control registers.

Transmit Address Space	Address(14:13)
Secure Channel CAM and data	00
Encryption Unit Key Memory	01
SecY Statistics Memory	10
Global Control Registers	11

Table 6: MACSec Transmit Channel and Global Resources Address Space.

Receive Channel Resources

Secure Channel CAM and Replay Counters

Each Secure Channel has a 64 bit Secure Channel Identifier (SCI) associated with it, this is split into a 32 bit Most Significant Word (MSW) and Least Significant Word (LSW). An SCI of 0xFFFFFFFF can be written to hardware channels which are not in use to prevent spurious matches, this value is specified in IEEE802.1ae as never occurring in a legal packet. The SCI from the incoming packet SecTag is matched with values in the CAM in order to find the correct SC and this is then further indexed using the AN from the packet header to determine the SA and the key to decode the packet. Address bits(12:7) select one of 64 Secure Channels.

The SCI from receive channel 0 is used as the default SCI when the MACSec core is used in a point to point link and the MACSec packets do not include an explicit SCI.

The SA in Use Mask and SecY index mask word has two functions: bits(3:0) are the AN in use mask determine whether the corresponding SA for this SC is in use (i.e. bit 0 = 1 means SA 0 is in use). Bits (6:4) are used to hold the 3 bit index of the SecY with which this SC is associated.

The Lowest Acceptable PN and Next PN fields track packet numbers in order to detect replay attacks using the algorithm in Figure 10-5 of the IEEE 802.1AE standard. These resources are associated with a Security Association where the first three resources are associated with a Secure Channel. Address bits (6:5) select one of four Security Associations for each channel.

Receive Secure Channel CAM Address Space	Address(12:7)	Address(6:5)	Address(4:0)
SCI MSW	SC	00	00000
SCI LSW	SC	00	00001
SA In Use Mask and SecY Index	SC	00	00010
Lowest Acceptable PN	SC	AN	00100
Next PN	SC	AN	00101

Table 7: Secure Channel CAM and Replay Counter Memory.

Decryption Unit Key Memory

Each MACSec Secure Channel (SC) has 4 Security Associations (SA) associated with it. Some of these SAs may be marked as inactive using the AN In Use mask in the secure channel CAM. The MACSec IP core supports 64 SCs and therefore has 256 SAs: this number can be increased at the expense of additional FPGA resources with minor changes to the code. Each of the SAs has an associated key. The MACSec IP core can be configured to support 256 bit keys as well as the 128 bit keys specified in IEEE802.1ae: 256 bit keys are required to protect classified data in defense applications.

Each SA channel has 8 words of memory for 256 bit keys and 16 words of memory for 256 bit keys. Memory is allocated sequentially starting with SC 0 and SA 0 at address 0. The MSW of the key data is in the lower address location (following the convention in the AES standards for indexing words within a word) so memory location 0 in this area will contain the MSW of the key for SC 0, SA 0.

The table provides for eight 128 bit blocks of data for each key (requiring 32 addressable locations). This key data is pre-calculated from the key using software provided by Algotronix, the pre-calculation increases the efficiency of the AES-GCM computation and reduces area compared with an implementation which was starting from the key itself. Specifics of the pre-calculated data will be provided under NDA.

Decryption Unit Key Memory Address Space	Address(12:7)	Address(6:5)	Address(4:0)
Precalculated Key Information	SC	AN	offset

Table 8: Decryption Unit Key Memory.

Receive SecY Statistics and Control Memory

This address space provides control registers to configure the SecY and SecY receive statistics not associated with a particular channel. Bits (5:3) select one of eight virtual SecYs and bits (2:0) a resource within that SecY as shown in Table 6. Bits 10:8 of the address bus should be set to 0 since they may be decoded in future versions of the core to allow for additional resources. These statistics registers and their functionality are defined in the 802.1AE standard.

The statistics counters are not cleared by the core reset signal and should be initialised to zero by the device driver.

Status Registers	Address(12:7)	Address(6:3)	Address (3 : 0)
Input Packets Untagged	000000	SecY	000
Input Packets No Tag	000000	SecY	001
Input Packets Bad Tag	000000	SecY	010
Input Packets Unknown SCI	000000	SecY	011
Input Packets No SCI	000000	SecY	100
Input Packets Overrun	000000	SecY	101
Input Octets Validated	000000	SecY	110
Input Octets Decrypted	000000	SecY	111

Table 9: Receive SecY Statistics and Control Memory

Security Association Statistics

The MACSec core keeps various statistics for each receive Security Association as specified in Figure 10-6 of the IEEE802.1ae standard. The MACSec hardware does not keep SC statistics directly but relies on the device driver software to calculate the SC statistics by summing across all SAs associated with the SC. Calculation of SC statistics by aggregating SA statistics rather than keeping them directly is explicitly allowed by the standard.

Bits (10:5) select one of 64 SCs, bits (4:3) select one of 4 SAs associated with that SC and bits (2:0) select one of 8 statistics variables associated with that SA as shown in Table 8.

Statistic Counter	Address(12:11)	Address(10:5)	Address(4:3)	Address (2:0)
Input Packets OK	00	SC	AN	000
Input Packets Un-checked	00	SC	AN	001
Input Packets Delayed	00	SC	AN	010
Input Packets Late	00	SC	AN	011
Input Packets Invalid	00	SC	AN	100
Input Packets Not Valid	00	SC	AN	101
Input Packets Not Using SA	00	SC	AN	110
Input Packets Unused SA	00	SC	AN	111

Table 10: Statistics variables associated with each receive SA.

Transmit Channel Resources

Transmit Destination Address CAM

Address space is provided for 64 entries in the CAM, this value was chosen to allow one entry for each of 64 SCs. The number of routing table entries actually implement within the available address space is specified by a separate constant (in macsec_package.vhd) from the constant specifying number of SCs implemented to allow area optimisation.

Each entry has a two word Destination Address (an Ethernet address is 48 bits long and the top 16 bits of the MSW address are not significant) for matching against the Destination Address in the incoming packet.

The corresponding virtual SecY is provided as a 4 bit number allowing for 16 Virtual SecYs.

If bit 0 of the 'In Use' word is 0 the CAM will not match independent of the destination address words.

In the case where the destination address does not match a CAM entry SecY 0 is returned as a default.

Transmit Destination Address CAM Address Space	**Address(12)**	**Address(11:8)**	**Address(7:2)**	**Address(1:0)**
Destination Address MSW (in bits(15:0))	0	0000	CAM Index	00
Destination Address LSW (in bits (31:0))	0	0000	CAM Index	01
In Use (bit 0)	0	0000	CAM Index	10
Index of corresponding SecY (in bits(3:0))	0	0000	CAM Index	11

Table 11: Transmit Destination Address CAM.

SecY Data Memory

There are 8 SecYs and a block RAM is used to provide the control information for each SecY, including information for the four SAs associated with the transmit SC. Some of the SecY control resources are associated with the receive channel.

SecY Data Memory	**Address(12)**	**Address[11:8]**	**Address(7:4)**	**Address(3:2)**	**Address(1:0)**
Transmit SCI MSW	1	0000	SecY	00	00
Transmit SCI LSW	1	0000	SecY	00	01
Control Word	1	0000	SecY	00	10
Transmit Next PN	1	0000	SecY	10	AN

Table 12: Transmit SecY Data Memory SA Entry.

SecY Control Word Format

This word within the SecY memory for the transmit channel consists of a set of bits (Table 14) which configure the core functionality, most of these bits correspond with variables in Figure 10-6 of the IEEE 802.1ae standard.

The Controlled Port Enable bit can be set to 0 by the user to disable the controlled port. The associated control signal can also be forced to 0 by the MACSec core itself to indicate that an error condition has occurred which has forced the controlled port to be disabled. The standard specifies the controlled port should be disabled when the transmit Next Packet Number counter is zero - this catches the condition where the counter has wrapped round. Therefore, it is possible for the control port to be disabled even when this user controlled bit is set to 1.

Function	**Bit**
Transmit AN	(1:0)
Controlled Port Enable (**volatile**)	2
Use ES	3
Use SCB	4
Multiple Active Receive Channels	5
Always Include SCI	6
Protect Frames	7
Transmit SA0 Confidentiality	8
Transmit SA1 Confidentiality	9
Transmit SA2 Confidentiality	10
Transmit SA3 Confidentiality	11
Validate Frames	(13:12)
Replay Protect	14

Table 14: Transmit SecY Control Word Bit Positions

The Controlled Port Enable bit for each SecY is also required by the transmit channel, at present it is envisaged that it will duplicated in the memory within the receive channel and the device driver will be required to write both copies. It is possible a more complex scheme will be required.

The two bit Receive Validate Frames field is encoded as follows: 00 = Disabled, 01 = Check, 10 = Strict. The actions for each value are defined in Figure 10-5 of the 802.1AE standard and are not exactly as might be expected from their names (e.g. a packet with a bad ICV and the C bit in the packet header true would still be dropped and the Not Valid counter incremented even if Validate Frames was Disabled).

Encryption Unit Key Memory

Each MACSec SecY has a single transmit Secure Channel (SC) which has 4 Security Associations (SA) associated with it. Each SA has a corresponding encryption key so the number of encryption keys is 4 times the number of SecYs.

Each SA channel has 8 words of memory for 256 bit keys and 16 words of memory for 256 bit keys. Memory is allocated sequentially starting with SC 0 and SA 0 at address 0. The MSW of the key data is in the lower address location (following the convention in the AES standards for indexing words within a word) so memory location 0 in this area will contain the MSW of the key for SC 0, SA 0.

The table provides for eight 128 bit blocks of data (thirty two addressable memory locations) for each key. This key data is pre-calculated from the key using software provided by Algotronix, the pre-calculation increases the efficiency of the AES-GCM hardware and reduces area compared with an implementation which was starting from the key itself. Specifics of the pre-calculated data will be provided under NDA.

Encryption Unit Key Memory Address Space	Address(12:11)	Address(10:7)	Address(6:5)	Address(4:0)
Pre-calculated Key Information	00	SecY	AN	offset

Table 13: Encryption Unit Key Memory.

Transmit SecY Statistics Memory

This address space provides control registers to configure the SecY and SecY receive statistics not associated with a particular channel. Bits (7:5) select one of eight virtual SecYs and bits (2:0) a resource within that SecY as shown in Table 7. Bits 10:8 of the address bus should be set to 0 since they may be decoded in future versions of the core to allow for additional resources.

Output Packets to Disabled Port is an additional statistics counter not specified in the standard which is provided by the core as a convenience since the core will drop packets in this scenario rather than halting until the port is enabled again. Stopping processing and leaving packets for a disabled SecY waiting to enter the core is not practical since there is only one input port shared between multiple SecYs and this would block traffic for the other SecYs as well as the disabled one.

Resource	Address(10:9)	Address (8:5)	Address(4:3)	Address (2 : 0)
Output Packets Untagged	00	SecY	AN	000
Output Packets Too Long	00	SecY	AN	001
Output Octets Protected	00	SecY	AN	010
Output Octets Encrypted	00	SecY	AN	011
Output Packets Protected	00	SecY	AN	100
Output Packets Encrypted	00	SecY	AN	101

Output Packets to Disabled Port	00	SecY	AN	110

Table 15: Transmit SecY Statistics

MACSec Global Control Registers

Global Control Register Address Space	Address (10:2)	Address (1:0)
Receive Channel Replay Window	000000000	00
MACSec ID Register	000000000	01

Table 16: Global Control Register Address Space within Transmit Channel

Receive Channel Replay Window

This register is used to determine the lowest acceptable packet number for received packets, if Replay Protect is enabled packets with a number lower than this value will be discarded (see IEEE802.1AE paragraph 10.6.4 and 10.6.5 and Figure 10.5 for an exact description of the replay detection mechanism).

MACSec ID Register

This register will read back as the constant hex value 0x416c676f which in ASCII is "Algo". Reading back this register is an easy way to check that the IP core has been correctly integrated into the host system.

Verification Methods

The testbench includes a self-checking configuration of the top level entity in the VHDL design which uses a behavioral model of MACSec to check the results from the synthesisable implementation code. This is implemented using the VHDL facility to provide multiple architecture definitions for a particular entity: the top level entity in the design has a self_checking and a synthesis architecture defined. As shown in Figure 5, the self checking architecture has an identical interface to the synthesisable architecture and instances the synthesisable architecture within itself but also contains behavioral code to capture all input and output signals and check their values against expected values computed using a behavioral model. When errors are detected assertions are triggered and the simulation is stopped with an error message.

This self-checking configuration of the MACSec core can also be instantiated within the user's own simulations. This makes it easy to verify the core operates properly when connected to the user circuitry surrounding the core. In addition, the assertions within the self checking code will detect and report many situations where the user design is not driving the core correctly simplifying the task of integrating the core with the larger user design easier.

The MACSec testbench supplied with the core stimulates the self checking core with a random sequence of packets, writes of key information and key activations and the self checking core takes responsibility for detecting any errors.

.

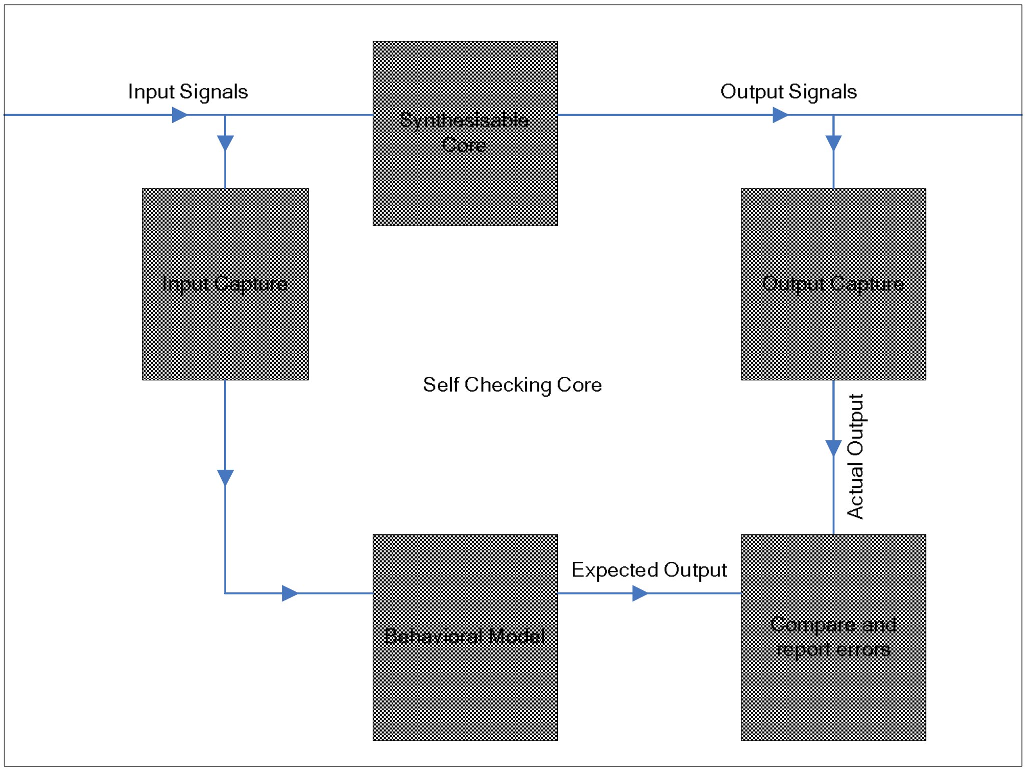

Figure 5, Multiple SecY MACSec Self Checking Architecture

The AES-GCM-10G core used within MACSec is also separately verified using its own testbench.

Recommended Design Experience

It is recommended that the user is familiar with the VHDL or Verilog language and with the Xilinx design flow and simulation tools. The coding standards used when creating the product allow automatic translation of the synthesisable core (but not the testbench code) into Verilog without loss of readability.

It is recommended that the user has a background in data security or takes appropriate advice when considering how to implement MACSec in a larger system.

Information on the MACSec Algorithm

MACSec Standards

MACSec is specified in IEEE standard 802.1AE (2006) the corresponding standard document can be obtained from the IEEE (www.ieee.org). The standard was updated in 2011 as 802.11AEbn to allow the use of 256 bit keys in AES-GCM.

The AES and AES-GCM algorithms used in MACSec are standardized by the Computer Security Division, National Institute of Standards and Technology (NIST), Gaithersburg MD. The relevant standard to this implementation is FIPS 197 which specifies the AES algorithm. The FIPS 197 document provides an excellent and concise description of the processing involved in implementing AES and therefore this basic information on the structure of the AES algorithm is not repeated here.

NIST Special Publication SP800-38D describes the AES-GCM algorithm, this document is derived from a proposal to NIST by Cisco..

These NIST documents can be downloaded free of charge from the NIST website (www.csrc.nist.gov).

Customization Service

Algotronix can offer a cost effective customization service for this core in order to tune the implementation for easy integration into a larger system or extend the product to meet particular requirements. It is also possible to produce variants with significantly higher performance at the expense of increased area and to create optimized variants of the core targeted at particular FPGA devices.

Algotronix is a registered trademark of Algotronix Ltd. in the United States and United Kingdom and a trademark of Algotronix Ltd. in other countries.

The supply of the product described in this document is the subject of a separate license agreement with Algotronix Ltd. which defines the legal terms and conditions under which the product is supplied. This product description does not constitute an offer for sale, a warranty of any aspects of the product described or a license under the intellectual property rights of Algotronix or others. Algotronix products are continuously being improved and are subject to change without notice. Algotronix products are supplied 'as is' without further warranties, including warranties as to merchantability or suitability for a given purpose. Algotronix products are not intended for use in safety critical applications.

This cryptographic product is subject to export control. It is freely available within the European Union and can be supplied immediately to Australia, Canada, Japan, New Zealand, Norway, Switzerland and the United States under Community General Export Authorisation EU001.

Export to other countries requires an export licence. The UK Department of Business, Enterprise and Regulatory Reform publishes information on their website (www.berr.gov.uk) which gives an indication of average export licence processing times for various countries and the percentage of licence requests which are granted. For many countries obtaining an export licence can be done relatively quickly and with only a small amount of additional paperwork.

It is the the responsibility of the customer to comply with all applicable requirements with respect to re-export of products containing the AES technology.

Algotronix Ltd.
130-10 Calton Road
Edinburgh EH8 8JQ
Phone: +44 131 556 9242
E-mail: cores@algotronix.com

URL: www.algotronix.com

Version Control Information	
Subversion Revision Number	75
Date	2015/09/21 15:07:01
Document	Macsec 40g Data Sheet, Platinum Edition
Status (blank field indicates OK/no warnings)	
	(Table auto-updates, do not edit field values by hand)