XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

SECURITY WITH TIMING ACCURACY: PTP SUPPORT WITH MACSEC IP CORE

White Paper

Kimmo Järvinen, CTO, Xiphera Ltd
Tuomo Tarvainen, System Architect, Xiphera Ltd
Matti Tommiska, CEO, Xiphera Ltd
info@xiphera.com

White Paper
ver. 1.0
March 2, 2022

Contents

1 Introduction and problem statement 2

2 Review of the relevant O-RAN standards and their applicability to MACsec and PTP 2

3 Overview of Intel® Agilex™ FPGA architecture and Precision Time Protocol support 3
3.1 Precision Time Protocol 3
3.2 Intel® Agilex™ E- and F-tiles and PTP support 4

4 Description of MACsec 5
4.1 MACsec frame format 5
4.2 AES-GCM as the cipher engine in MACsec 6

5 Xiphera's MACsec IP cores and PTP support 8

6 Summary 9

ABSTRACT

The O-RAN ALLIANCE aims to standardize open interfaces enabling multi-vendor Radio Access Network (RAN) deployments. Both the security of the open interfaces, specifically Open Fronthaul (FH), and the accuracy of timing information must be guaranteed. Both of these requirements can be met with Xiphera's MACsec Intellectual Property (IP) cores when implemented on Intel® Agilex™ FPGAs.

1 Introduction and problem statement

The first 5G networks have been single-vendor solutions, and telecom operators have had a limited number of suppliers to choose from when deciding where to obtain all the network components. The mission of the O-RAN ALLIANCE since its foundation in February 2018 has been to drive the telecommunications industry towards more intelligent, open, virtualized and fully interoperable mobile networks. The benefits of this approach include expanding the ecosystem, fostering competition and innovation between different OEMs, and enabling newcomers to enter the growing RAN market. However, the potential security risks of the open RAN must be addressed proactively, and the confidentiality, integrity and authenticity of all four signalling planes (Control, User, and Synchronization (CUS) and the Management (M)) on the open interfaces of the O-RAN network architecture must be standardized and supported. This is especially true for the Open FH connection between Distributed Unit (DU) and Radio Unit (RU), and an unsecured Open FH is a potential attack vector.

A well-known security protocol to address the security challenges is MACsec. Providing correct timing information is also critical on fronthaul connections, and the IEEE 1588 Precision Timing Protocol (PTP) is commonly used for this purpose. This adds another dimension to the eventual security protocol because in addition to securing the messages, it must also guarantee deterministically measurable transmission of timing-critical synchronization messages. As the well-known features of Field Programmable Gate Arrays (FPGA) include low processing latency and high throughput, they are natural candidates for MACsec implementations with PTP support in an O-RAN architecture.

This White Paper is structured as follows: First, the current state of relevant O-RAN standards is reviewed. This is followed by an overview of the Intel® Agilex™ FPGA architecture and its support for the PTP protocol. The MACsec protocol is presented, and its underlying cryptographic algorithms are explained at a high level. The processing of Synchronization messages differs from the processing of Control and User plane messages, and the architecture to accomplish this with an Intel® Agilex™-based implementation of Xiphera's MACsec solution is presented. The White Paper is concluded by a summary.

2 Review of the relevant O-RAN standards and their applicability to MACsec and PTP

The O-RAN standardization is based on the work done by 3GPP, and the standardization work is divided into ten Working Groups (WG). Additionally, there are two focus groups, Test & Integration Focus Group (TIFG), and more importantly for the topic of this White Paper, Security Focus Group (SFG).

O-RAN ALLIANCE has defined a total of eleven interfaces that are used within a RAN. Three of these open interfaces, along with the overall O-RAN architecture, are presented in Figure 1. These interfaces are the Backhaul (that connects the RAN to the Core network), Midhaul (that connects the Centralized Unit (CU) and the DUs), and Fronthaul (that connects the RUs and DUs).

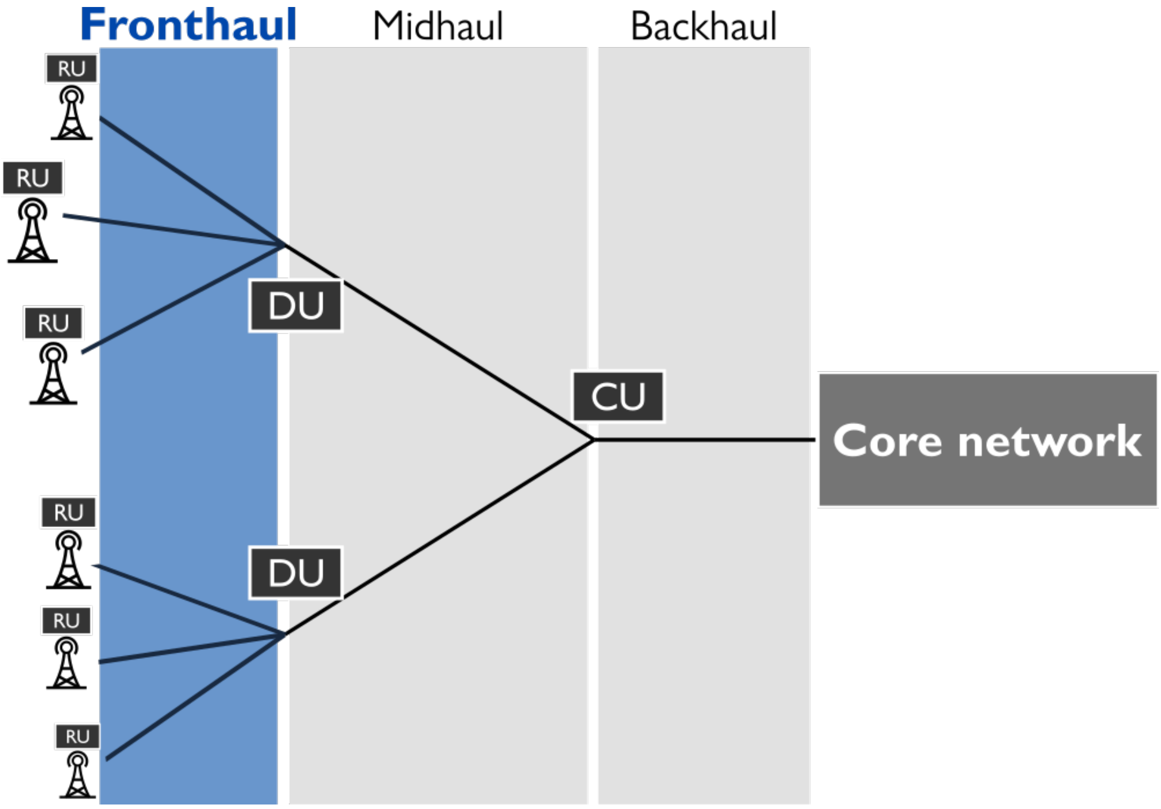


Figure 1: Overview of O-RAN architecture

3 Overview of Intel® Agilex™ FPGA architecture and Precision Time Protocol support

Intel® Agilex™ FPGAs are built on Intel's 10nm FinFET process, and they are based on a chiplet architecture, which enables the integration of heterogeneous technology elements in the same package. This is also known as System-in-Package (SiP). Additionally, by leveraging advanced 3D packaging technology (for example, Intel Embedded Multi-Die Interconnect Bridge (EMIB)), a traditional FPGA die can be combined with special-purpose semiconductor dies to create devices that are optimized for specific target applications. An overview of the Intel® Agilex™ architecture is presented in Figure 2.

One example of the possibilities provided by the chiplet architecture is the integration of different types of transceiver tiles with the FPGA fabric. This White Paper focuses on the PTP features offered by Intel® Agilex™ E- and F-tiles.

3.1 Precision Time Protocol

The Precision Time Protocol (PTP) is formally defined in the IEEE Standard 1588-2019. The two main use cases of the PTP protocol are the synchronization of clocks between communication nodes and the measurement of propagation delays between communication nodes.

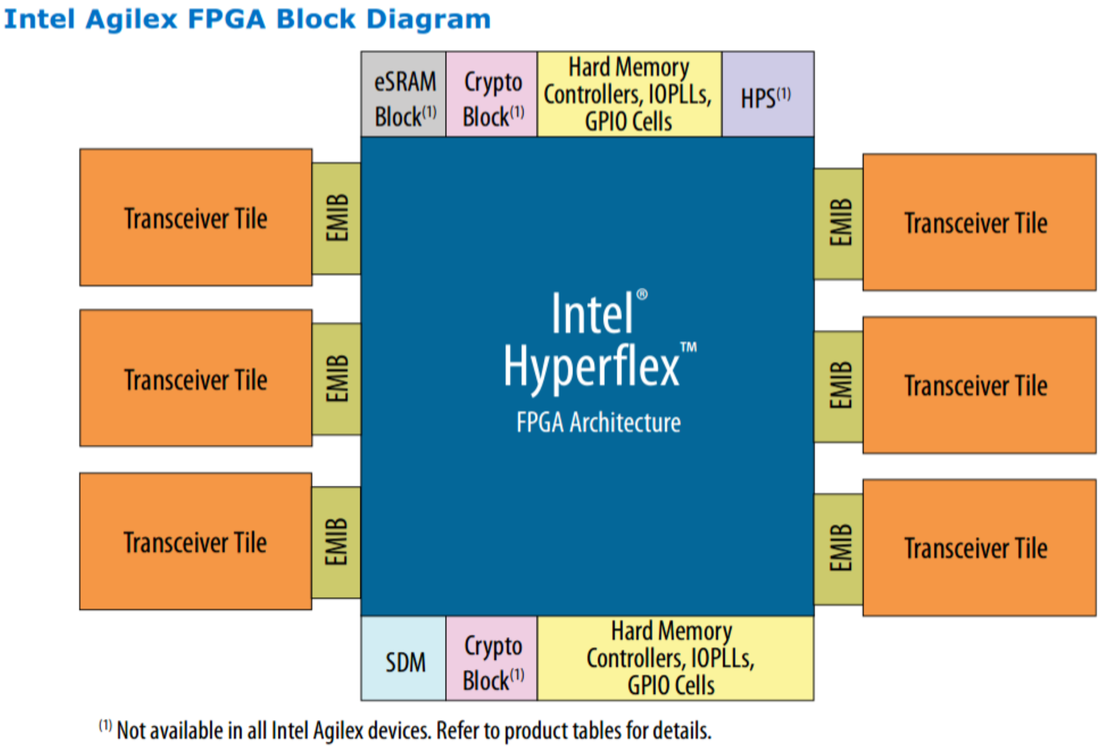

Intel Agilex FPGA Block Diagram
eSRAM Block(1)
Crypto Block(1)
Hard Memory Controllers, IOPLLs, GPIO Cells
HPS(1)
Transceiver Tile
EMIB
Transceiver Tile
EMIB
Transceiver Tile
EMIB
Intel® Hyperflex™ FPGA Architecture
EMIB
Transceiver Tile
EMIB
Transceiver Tile
EMIB
Transceiver Tile
SDM
Crypto Block(1)
Hard Memory Controllers, IOPLLs, GPIO Cells
(1) Not available in all Intel Agilex devices. Refer to product tables for details.

Figure 2: Intel® Agilex™ FPGA architecture

The requirements for timing accuracy are in their part defined in the standard ITU-T G.8273.2/Y.1368.2, and the four timing accuracy classes are outlined in Table 1.

Class	Timing accuracy
A	100ns
B	70ns
C	30ns
D	5ns

Table 1: Precision Time Protocol Accuracy Classes

The synchronization in the PTP protocol is accomplished by adding time stamps into transmitted Ethernet frames, and subsequently checking local time when the time stamped frames arrive at the receiving end. The extracted information makes it possible to calculate both frequency offset and propagation delays. There are two main ways to accomplish this, namely PTP 1-step and PTP 2-step. Their timing diagrams are presented in Figure 3. It should be noted that in the PTP 2-step case, t_{1k} is captured when the `Sync` message is actually transmitted. The actual timestamp is sent with the `Follow_up` message after the `Sync` message.

3.2 Intel® Agilex™ E- and F-tiles and PTP support

Both E- and F-tiles in the Intel® Agilex™ FPGA with Ethernet MAC Hard IP support PTP in both 1-step and 2-step mode. The PTP support can be configured either in the basic mode or in the advanced mode, and the timestamp accuracy with E- and F-tiles varies from +/-1.5ns to +/-8ns depending on the mode and linespeed.

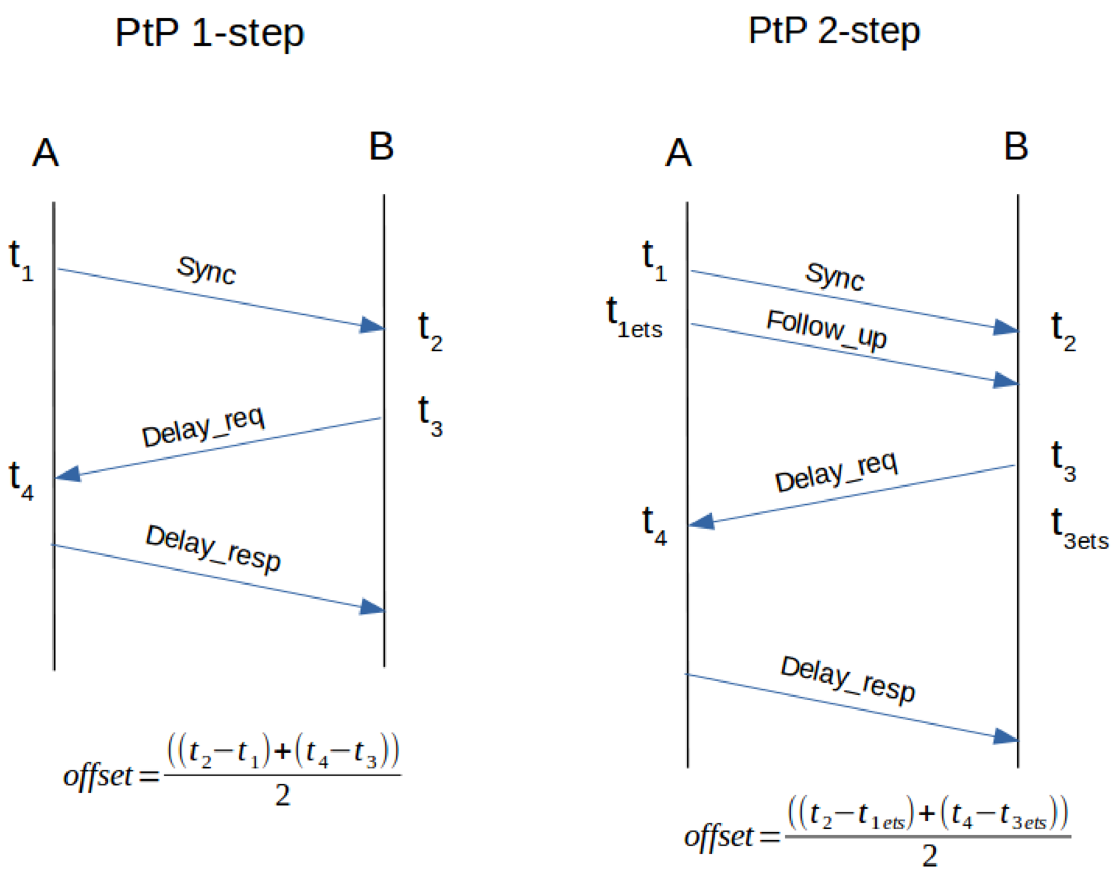


Figure 3: PTP 1-step and 2-step flow

As an example of the receiver (Rx) side PTP functionality in Intel® Agilex™ FPGA, each received packet is timestamped with the timing information derived from the local Time of Day (ToD) block in the transceiver. The Rx timestamp value is valid when a valid `startofpacket` (SoP) signal is active, and the timestamp is presented in 96-bit mode, supporting timestamp resolution downto $1/2^{16}$ns (15.25 fs). A block diagram of the E-tile PTP receive functionality is presented in Figure 4.

4 Description of MACsec

The MACsec protocol is formally defined in IEEE Std 802.1AE-2018. It defines a security infrastructure for Layer 2 (as per the OSI model) traffic by verifying that a received frame has been sent by the transmitting station that claimed to send it. Furthermore, the traffic between the stations is both encrypted and authenticated to ensure data confidentiality and integrity. The MACsec protocol uses AES-GCM (Advanced Encryption Standard, Galois Counter Mode, see Section 4.2) with either 128-bit or 256-bit keys. The AES datapath width is 128 bits with both key lengths.

4.1 MACsec frame format

The MACsec frame format is presented in Figure 5. The functionality of a MACsec block in both the transmit and receive directions is based on the source MAC address (Src addr).

In the transmit direction the necessary parameters for performing the AES-GCM encryption and authentication are fetched from a lookup table indexed by the source MAC address. The

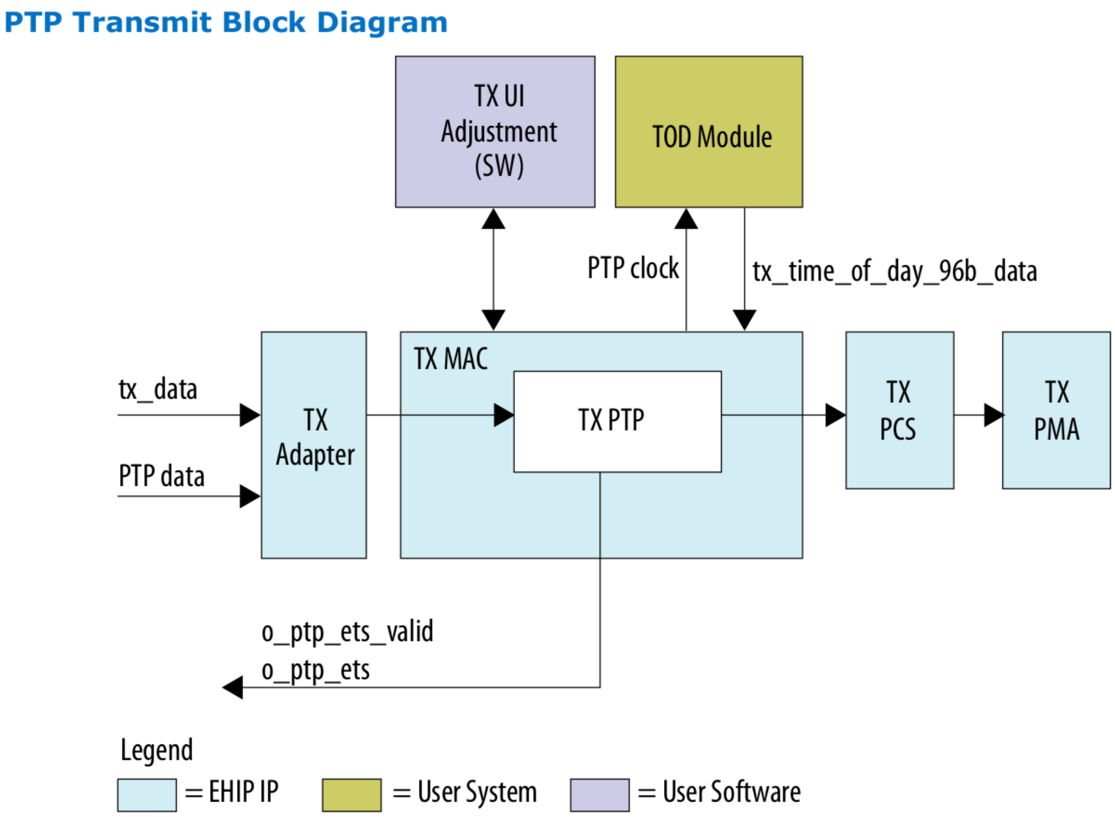


Figure 4: PTP receive functionality in Intel® Agilex™ FPGA E-tile

contents of the SecTAG field in MACsec frame are defined by these parameters, namely Tag Control Information (TCI), Association Number (AN), Packet Number (PN) and optional Secure Channel Identifier (SCI). Additionally, PN is incremented for each transmitted packet on each secure channel, and the packet length is checked for eventual updating of the short length (SL) field. The Initialization Vector (IV) for the AES-GCM algorithm is generated based on the parameters returned from the lookup function. The C and E flags in the TCI parameter define whether the payload data is both encrypted and authenticated, or only authenticated. The Integrity Check Value (ICV) returned by the AES-GCM algorithm is appended to the end of the message.

In the receive direction the source MAC address is used to fetch the required keys for the received packet. The IV value is generated based on the parameters in the received SecTAG. Again, depending on the parameters within the SecTAG, the received data is either decrypted and authenticated or only authenticated. In both cases, the authentication is accomplished by comparing the received and generated ICV values, and the received MACsec frame is accepted only if the values are the same.

4.2 AES-GCM as the cipher engine in MACsec

MACsec offers two cipher suites for protecting data in transmission: AES-GCM with 128-bit keys and AES-GCM with 256-bit keys. This section introduces AES-GCM and its building blocks, and discusses how AES-GCM can be implemented in hardware efficiently and how it is used in MACsec.

AES-GCM is an encryption scheme for authenticated encryption with associated data, which means that it offers simultaneous protection of data confidentiality and data authenticity. Confidentiality protection ensures that adversaries cannot find out any information about the true

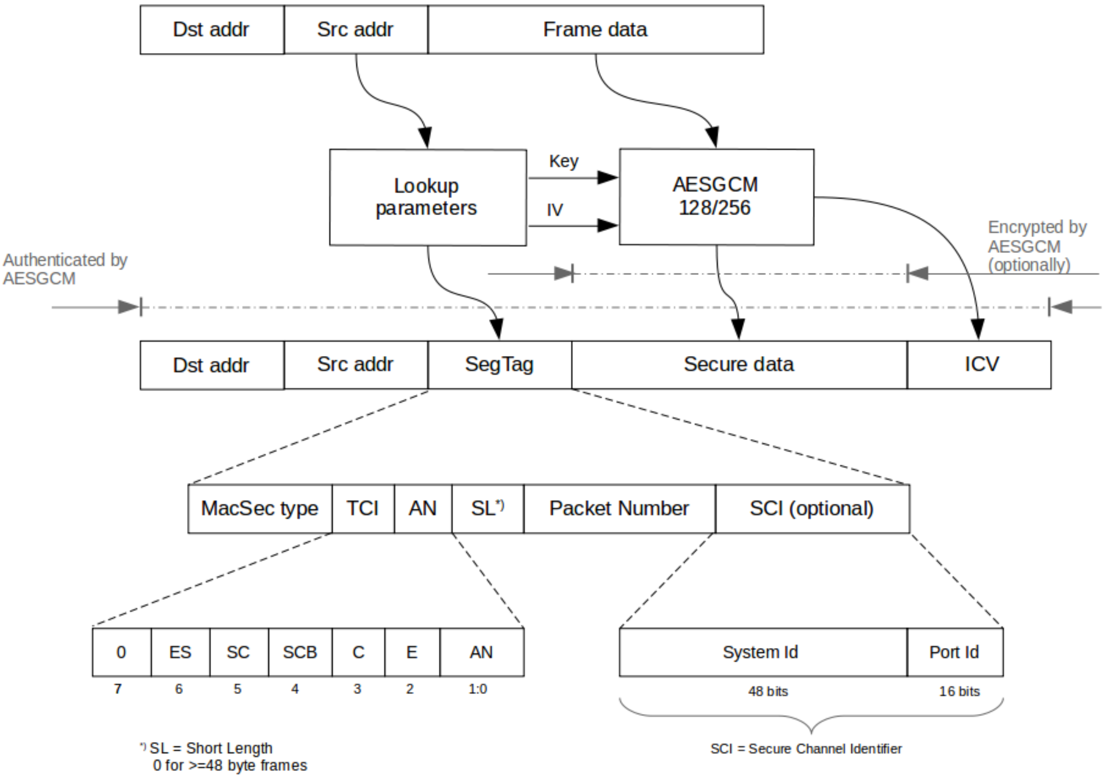


Figure 5: MACsec frame format

contents of the communication (besides certain obvious facts such as the length). Authenticity protection protects the data from manipulation and allows the receiver to get verification that the data was sent by the claimed sender. The term ”associated data” means that AES-GCM permits the use of associated data, which is a part in the communicated data that is protected only for authenticity. That is to say, associated data is sent in plaintext format without encrypting it, but it is still protected from any manipulation. A typical example of associated data is the header of a message, which must be sent unencrypted, for example, to allow routing of the message to the correct receiver. Internally AES-GCM combines AES in CounTeR (CTR) mode and Galois Message Authentication Code (GMAC) as shown in Figure 6.

AES-CTR can be implemented in hardware very efficiently for two reasons:

1. The AES computations can be fully pipelined because they do not have any dependency from previous computations.
2. Only AES encryptions are needed for both AES-GCM encryptions and decryptions, and consequently there is no need to support AES decryptions which are slightly more complicated compared to AES encryptions in hardware implementations.

GMAC is a message authentication code that takes a 128-bit authentication key and a message as inputs and returns a 128-bit authentication tag as an output. Similarly to other message authentication codes, GMAC works by having the sender of a message use GMAC with a specific key to compute an authentication tag (called ICV in the MACsec protocol) that is attached to the message. When the receiver receives the message and the authentication tag, it uses the same key and the received message to compute another GMAC tag. If the received tag and the computed tag are the same, then the receiver verifies that it received the authentic message. If the tags are

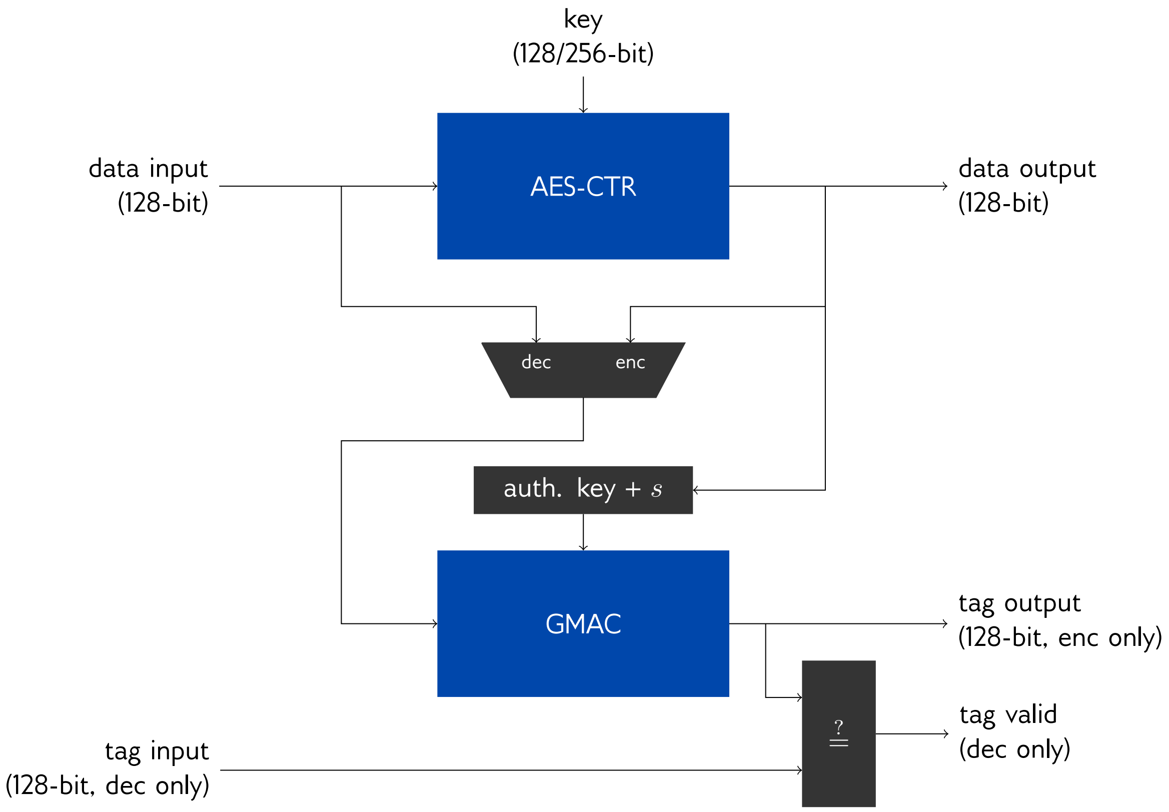


Figure 6: Structure of AES-GCM

different, it means either the message or the tag has changed during transmission. Because of the cryptographic properties of GMAC, an adversary, who does not have the key, cannot forge a message-tag pair that would pass this verification.

GMAC is more challenging to implement efficiently in hardware than AES-CTR, but with certain precomputations that permit parallel and/or pipelined processing. it can also be implemented in a way that it allows the processing of a new 128-bit block per clock cycle with high clock frequency.

In the case of MACsec, the header of the Ethernet frame that has been extended with MACsec specific fields is used as the associated data for AES-GCM. It is therefore protected for authenticity. Only the payload of the Ethernet frame is encrypted to protect its confidentiality. When MACsec is set to protect only authenticity, also payload is treated as associated data in the AES-GCM computation and there is no AES-GCM payload. An important aspect of MACsec is that it is impossible to modify the message payload or the header of the Ethernet frame after it has been processed with AES-GCM. In the case of PTP, this means that the time stamp must be inserted into the Ethernet frame before AES-GCM computation, and the latency of AES-GCM (and other processing after that) must be anticipated and included in the time stamp that is then sent to AES-GCM.

5 Xiphera's MACsec IP cores and PTP support

Xiphera supports the MACsec protocol with four Intellectual Property (IP) cores: XIP1211B, XIP1211H, XIP1213B, and XIP1213H. The last letter in the product code denotes the throughput (B = Balanced, targets single Gbps throughput; H = High-Speed, targets 25/50 Gbps throughput), and the last digit denotes the AES-GCM key length ('1' = AES128-GCM, '3' = AES256-GCM). XIP1213H, the high-speed

AES256-GCM IP core is used as an example for PTP support in the RX and Tx directions in the following sections.

Rx direction

When the XIP1213H core receives MACsec packets containing PTP messages, the Rx-side E/F tile (as described previously) set the ingress timestamps for each packet. The XIP1213H IP core can have several received packets in queue, and therefore the timestamps received from the EMAC need to be aligned with the packets from the XIP1213H IP core. This can accomplished with a FIFO-based implementation (See Figure 7), or alternatively with a streaming bus side channel.

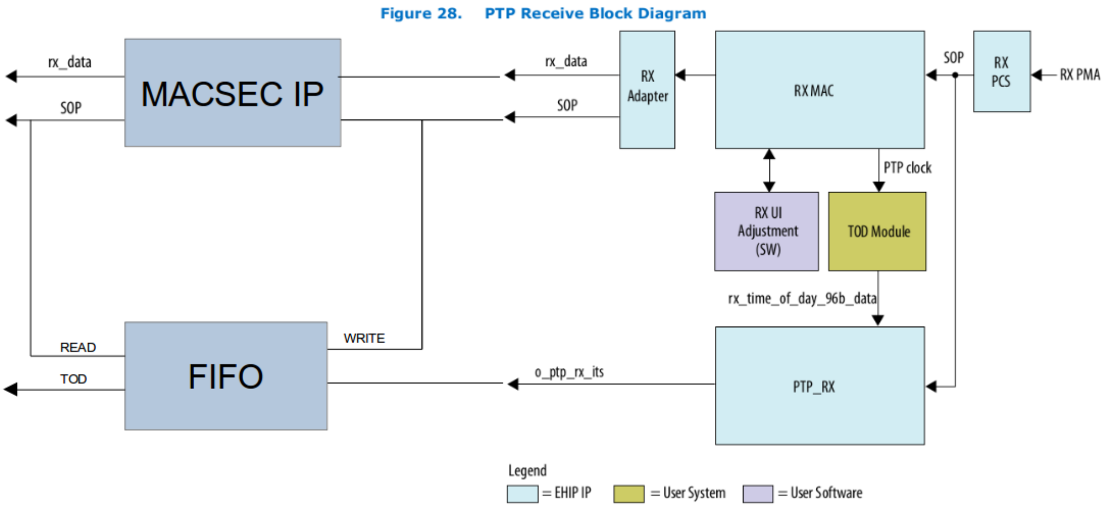


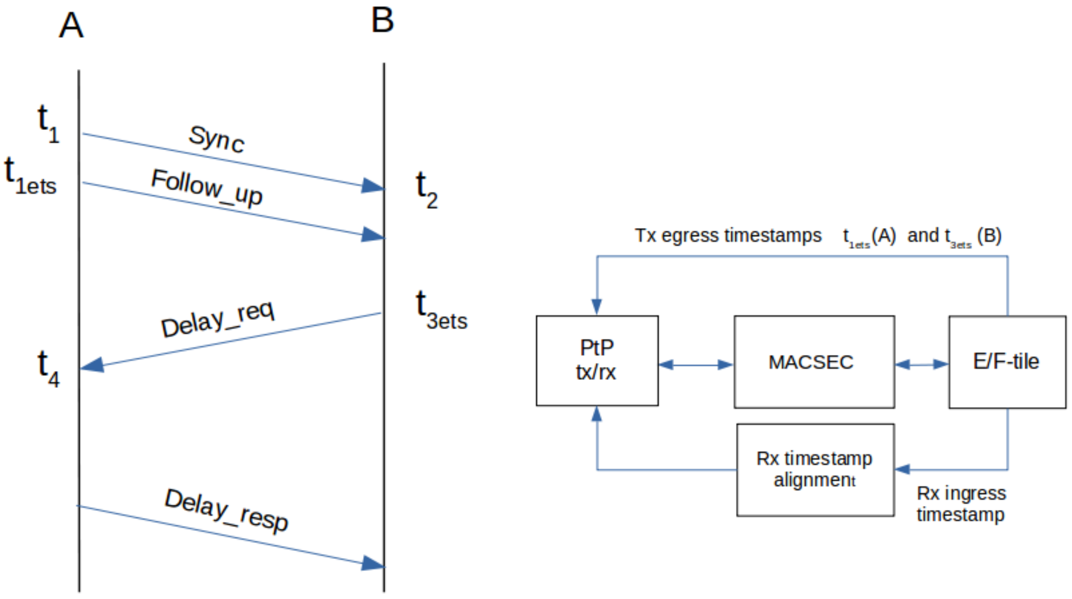
Figure 7: MACsec IP core (XIP1213H) in Rx direction on Intel® Agilex™ FPGA

Tx direction

When the XIP1213H IP core transmits PTP messages that are authenticated and optionally encrypted, the 2-step mode is used for both `Sync` and `Follow_up` messages. This is illustrated in Figure 8 as both a timeflow diagram and a high-level block diagram . At the A side, the `Follow_up` message uses the captured egress timestamp from the previously sent `Sync` message. Similarly, at the B side the t_3 timestamp for `Delay_req` message is captured from egress timestamp output of the E/F tile . When the `Delay_resp` message is received at the B side, both the frequency offset and the Rx and Tx latencies between A side and B side can be calculated.

6 Summary

The O-RAN architecture and its open interfaces are currently being standardized, and the MACsec protocol is a strong candidate for providing the required security (confidentiality, integrity and authenticity) for the latency-critical Open Fronthaul interface. The ability to combine the security of the Synchronization message based on the Precision Time Protocol (PTP) with the deterministically measurable latency is specifically important.



$$offset = \frac{((t_2 - t_{1ets}) + (t_4 - t_{3ets}))}{2}$$

Figure 8: PTP 2-step timing diagram and PTP functionality in Rx and Tx direction

Intel® Agilex™ FPGAs are based on a chiplet architecture, and the transceiver technical features of the E- and F-tiles enable support for the PTP protocol. This White Paper has presented a high-level overview on the methodology by which Xiphera's MACsec Intellectual Property (IP) cores can support PTP functionality with tens of gigabits of throughput per a single IP core on Intel® Agilex™ FPGAs.

References

[1] Joo Yeon Cho, Andrew Sergeev, and Jim Zou, "Securing Ethernet-based Optical Fronthaul for 5G Network", *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19)*, 2019

[2] D. Dik and M. S. Berger, "Transport Security Considerations for the Open-RAN Fronthaul", *2021 IEEE 4th 5G World Forum (5GWF)*, 2021

[3] E-tile Hard IP User Guide: E-Tile Hard IP for Ethernet and E-Tile CPRI PHY Intel® FPGA IPs, https://www.intel.com/content/dam/altera-www/global/en_US/pdfs/literature/ug/ug20160.pdf

[4] F-Tile Ethernet Intel® FPGA Hard IP User Guide, https://cdrdv2.intel.com/v1/dl/getContent/711705?fileName=ug20313-683023-711705.pdf

[5] G.8273.2: Timing characteristics of telecom boundary clocks and telecom time slave clocks for use with full timing support from the network, https://www.itu.int/rec/T-REC-G.8273.2/en

[6] IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security, IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006).

[7] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE 1588-2019, https://standards.ieee.org/standard/1588-2019.html

[8] Intel® Agilex™ FPGAs and SoCs Device Overview, https://www.intel.com/content/www/us/en/docs/programmable/683458/current/fpga-and-soc-device-overview.html

[9] Interview with Nagendra Bykampadi, New O-RAN ALLIANCE Security Focus Group Co-Chair, https://www.altiostar.com/interview-with-nagendra-bykampadi-new-o-ran-allaince-security-focus-group-co-chair/

[10] Morris J. Dworkin, SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Technical report, Gaithersburg, MD, United States, 2007.

[11] Open RAN explained, https://www.nokia.com/about-us/newsroom/articles/open-ran-explained/

[12] Security considerations of Open RAN, https://www.ericsson.com/en/security/security-considerations-of-open-ran

[13] Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001