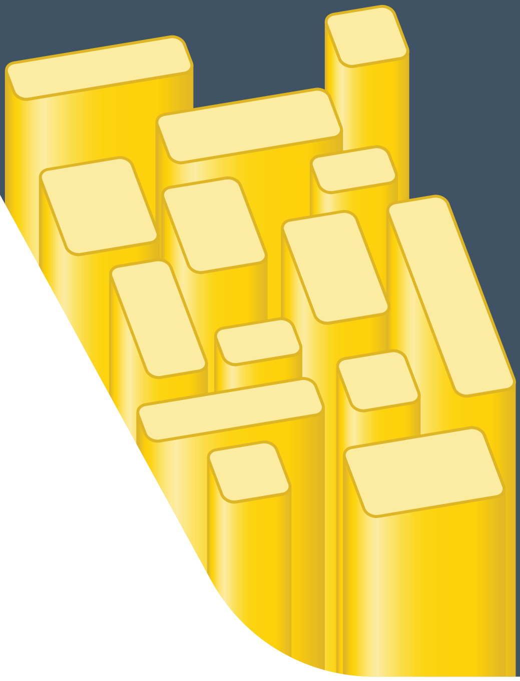
BittWare a molex company

Partner IP



XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

MACsec

IEEE 802.1AE IP Core

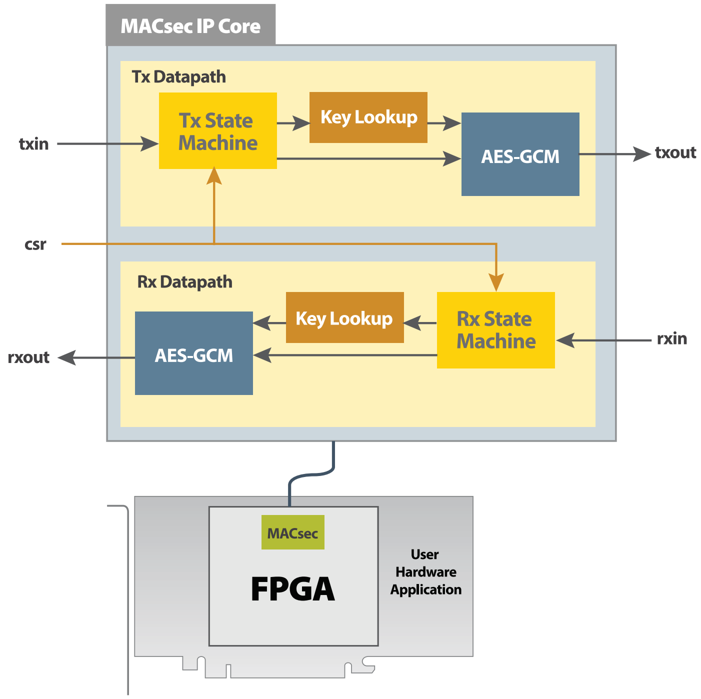
The Xiphera MACsec family provides high-speed IP cores implementing the MACsec (Media Access Control security) protocol as standardized in IEEE Std 802.1AE-2018. The MACsec protocol defines a security infrastrucure for Layer 2 (as per the OSI model) traffic by assuring that a received frame has been sent by a transmitting station that claimed to send it. The traffic between stations is also encrypted to provide data confidentiality and authenticated to provide data integrity.

Typical MACsec applications require high data bandwidths such as 10G, 25G, 40G, or 100G and often benefit greatly from FPGA-based acceleration. The Xiphera MACsec IP runs on BittWare's IA-840f and IA-420f Agilex FPGA-based PCIe cards.

Complies with IEEE std 802.1AE-2018

127.21 Gb/s in Altera Agilex F-series

Compliant with MACsec protocol



Features

Moderate resource requirements:

- The Xiphera MACsec IP (XIP1213E) requires 218238 Adaptive Lookup Modules (ALMs) (Altera ® Agilex ® F)

Performance:

- The Xiphera MACsec IP (XIP1213E) achieves a throughput in the 100 Gbps range, for example 127.21 Gbps in Altera® Agilex® F

Standard Compliance:

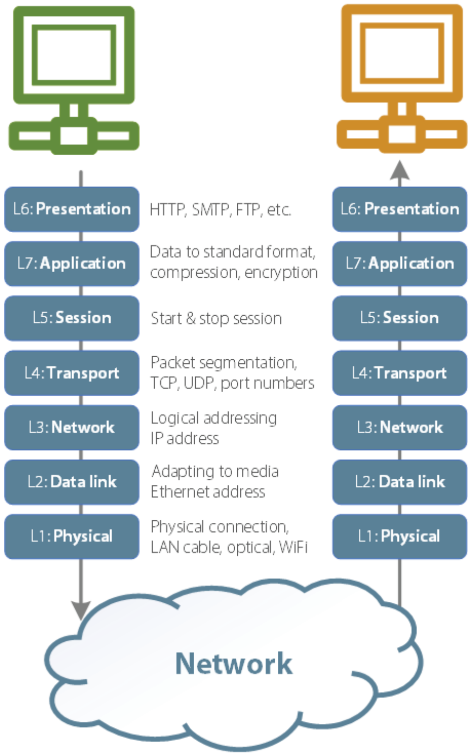
- The Xiphera MACsec IP is compliant with the MACsec protocol as standardized in IEEE Std 802.1AE-2018
- The cipher suite is fully compliant with the Advanced Encryption Algorithm (AES) standard, as well as with the Galois Counter Mode (GCM) standard

Test Vector Compliance:

- The Xiphera MACsec IP passes the test vectors specified in Annex C of IEEE Std 802.1AE-2018

MACsec

IEE 802.1AE IP Core

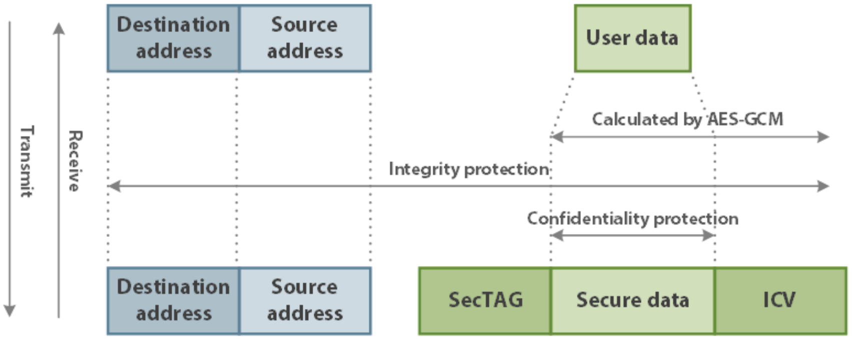


L6: Presentation
HTTP, SMTP, FTP, etc.
L7: Application
Data to standard format, compression, encryption
L5: Session
Start & stop session
L4: Transport
Packet segmentation, TCP, UDP, port numbers
L3: Network
Logical addressing IP address
L2: Data link
Adapting to media Ethernet address
L1: Physical
Physical connection, LAN cable, optical, WiFi
Network

OSI Network Model

Functionality

The Xiphera MACsec IP uses Advanced Encryption Standard with a 256-bit key in Galois Counter Mode (AES-GCM) to protect data confidentiality, data integrity and data origin authentication. XIP1213H is best suited for data traffic on 25 Gbps links, and XIP1213E is suited for traffic on 100Gbps links.

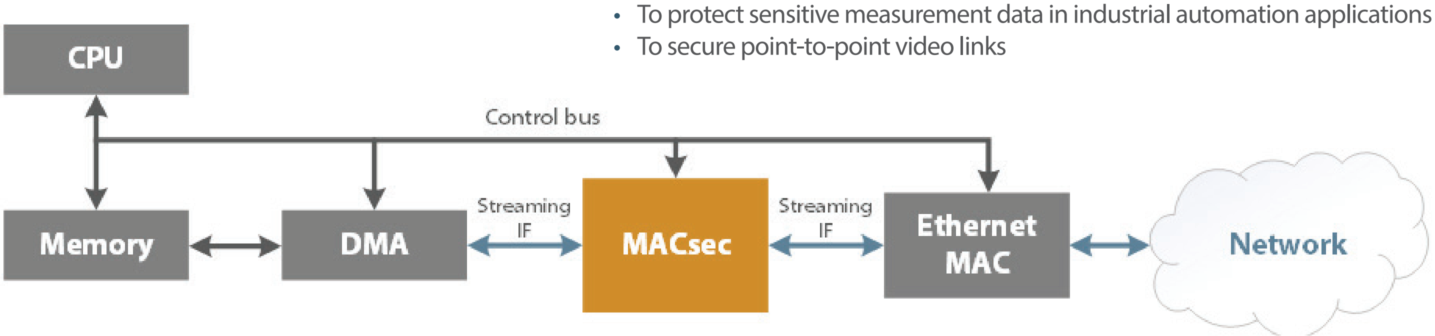


MACsec Frame Structure

Use Cases

The original use case for MACsec is protecting communications in wired local area networks. MACsec can also be used for the following:

- To protect critical control messages in communications networks
- To protect sensitive measurement data in industrial automation applications
- To secure point-to-point video links



MACsec IP Use Case

Deliverables

Encrypted source code, a comprehensive VHDL testbench and a detailed datasheet are included. The MACsec IP is available in three variants:

RS-XI-1213B	MACsec AES256-GCM
RS-XI-1213H	MACsec AES256-GCM, high-speed
RS-XI-1213E	MACsec AES256-GCM extreme-speed

Compatible FPGA Cards

- IA-840F
- IA-420F

Looking for a different card? Ask us about other compatible card options

To learn more, visit **www.BittWare.com**

v1 2024.03.14

BittWare a molex company