BittWare
a molex company

Partner IP

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

MACsec
IEEE 802.1AE IP Core

Media Access Control Security IP Core

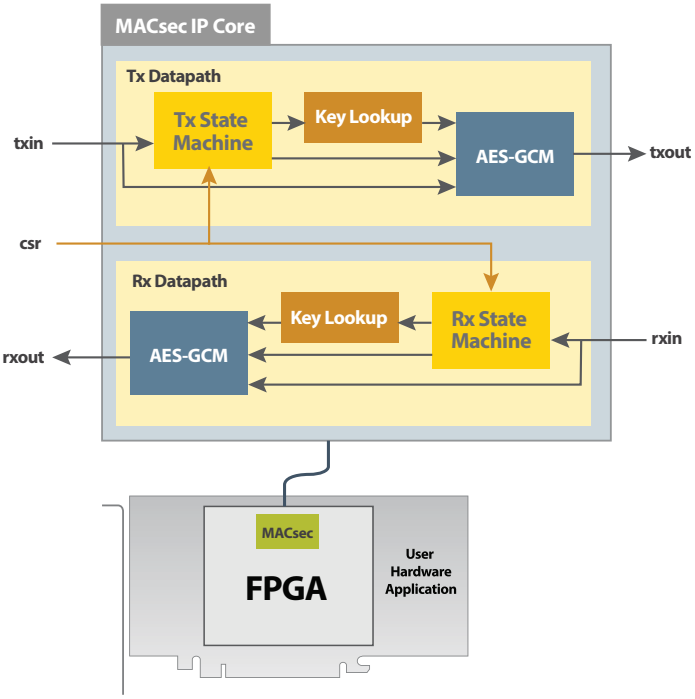
The Xiphera MACsec family provides high-speed IP cores implementing the MACsec (Media Access Control security) protocol as standardized in IEEE Std 802.1AE-2018. The MACsec protocol defines a security infrastrucure for Layer 2 (as per the OSI model) traffic by assuring that a received frame has been 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, or 40G 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.

Data confidentiality and integrity protection for the data link layer

key features

- Complies with **IEEE std 802.1AE-2018**
- **49.25+ Gb/s** in Intel Agilex F-series
- Fully compliant with **MACsec protocol**



Features

Moderate resource requirements:

- The Xiphera MACsec IP (XIP1213H) requires 53842 Adaptive Lookup Modules (ALMs) (Intel ® Agilex ® F)

Performance:

- The Xiphera MACsec IP (XIP1213H) achieves a throughput in the tens of Gbps range, for example 49.25+ Gbps in Intel® Agilex® F

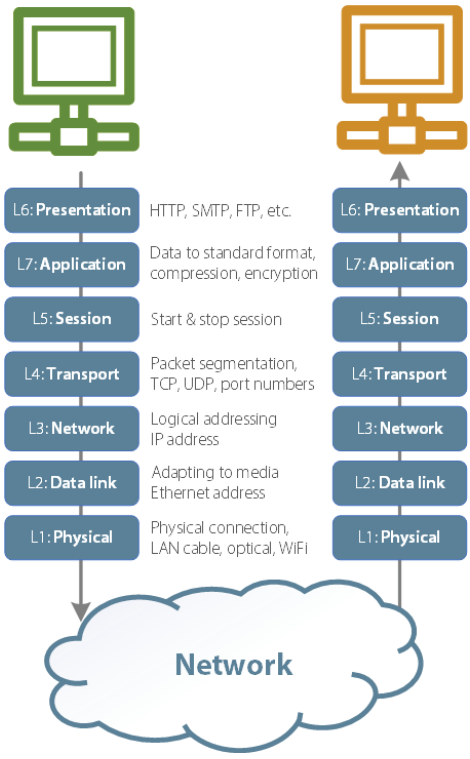
Standard Compliance:

- The Xiphera MACsec IP is fully 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

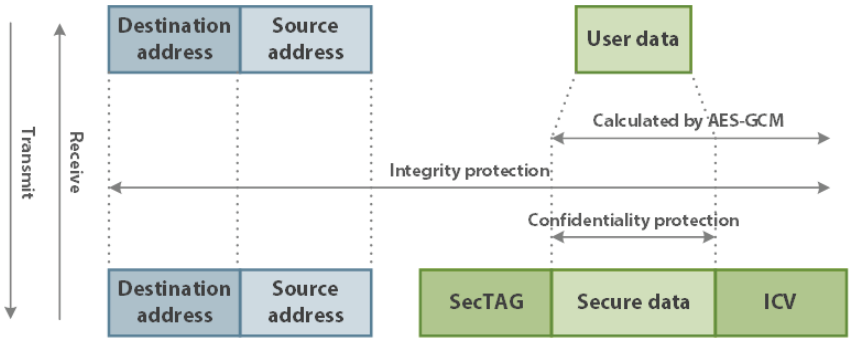
MACsec
IEE 802.1AE IP Core



OSI Network Model

Functionality

The Xiphera MACsec IP uses Advanced Encryption Standard with a 128 or 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.

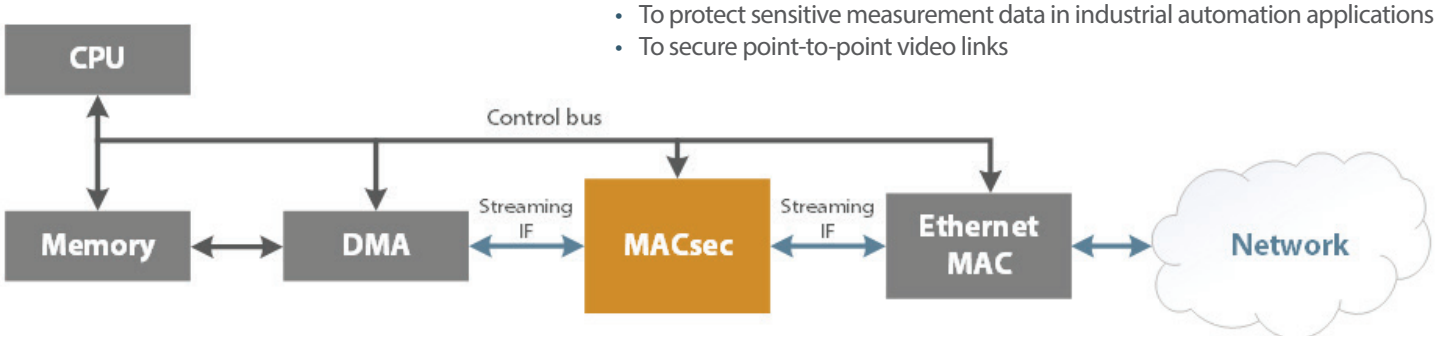


MACsec Frame Structure

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 four variants:

RS-XI-1211B	MACsec AES128-GCM
RS-XI-1211H	MACsec AES128-GCM, high-speed
RS-XI-1213B	MACsec AES256-GCM
RS-XI-1213H	MACsec AES256-GCM, high-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**

Rev 2022.4.20 | April 2022

BittWare
a molex company